Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 1.1

16-300698
Issue 2
September 2006

© 2006 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

http://www.avaya.com/support

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

http://support.avaya.com/ThirdPartyLicense/

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Security

See http://support.avaya.com/security to locate and/or report known vulnerabilities in Avaya products. See http://support.avaya.com to locate the latest software patches and upgrades. For information about secure configuration of equipment and mitigation of toll fraud threats, see the Avaya Toll Fraud and Security Handbook at http://support.avaya.com.

Contents

Chapter 1: Introduction 7
About This Guide 7
Differences Between 9600 Series and 4600 Series IP Telephones 8
Issue Date 9
What's New in Release 1.1 9
Document Organization 10
Other Documentation 10

Chapter 2: Administration Overview and Requirements 11
9600 Series IP Telephones 11
Parameter Data Precedence 14
The Administrative Process. 14
Administrative Checklist 15
Telephone Initialization Process 16
Step 1: Telephone to Network 16
Step 2: DHCP Server to Telephone 17
Step 3: Telephone and File Server 17
Step 4: Telephone and the Call Server 17
Error Conditions 18

Chapter 3: Network Requirements 19
Network Assessment 19
Hardware Requirements. 19
Server Requirements 20
DHCP Server 20
HTTP/HTTPS Server 20
Web Server (Optional) 20
Required Network Information 21
Other Network Considerations 22
SNMP 22
Reliability and Performance. 23
QoS 23
IEEE 802.1D and 802.1Q 23
Network Audio Quality Display on 9600 Series IP Telephones 24
IP Address Lists and Station Number Portability 24
TCP/UDP Port Utilization 25
Security 28
Registration and Authentication 28

Chapter 4: Communication Manager Administration 29
Call Server Requirements 29
Switch Compatibility and Aliasing IP Telephones 29
Media Server (Switch) Administration 30
IP Interface and Addresses 30
UDP Port Selection 30
RSVP and RTCP 31
QoS 31
IEEE 802.1D and 802.1Q 31
NAT 32
DIFFSERV 32
Voice Mail Integration 32
Call Transfer Considerations 32
Conferencing Call Considerations 33
Telephone Administration 34
Other Considerations 34

Chapter 5: Server Administration 35
Software Checklist 35
DHCP and File Servers 35
DHCP Server Administration 36
DHCP Generic Setup 36
Windows NT 4.0 DHCP Server 40
Verifying the Installation of the DHCP Server 40
Creating a DHCP Scope for the IP Telephones 41
Editing Custom Options 42
Adding the DHCP Option 42
Activating the Leases 43
Verifying Your Configuration 43
Windows 2000 DHCP Server 44
Verifying the Installation of the DHCP Server 44
Adding DHCP Options 46
Activating the New Scope 47
HTTP Generic Setup 47
HTTP Configuration for Backup/Restore 48
For IIS Web Servers 48
Web Configuration Tool 50

Chapter 6: Telephone Software and Application Files 53
General Download Process 53
Software 53
9600 Series IP Telephone Scripts and Application Files 54
Choosing the Right Application File and Upgrade Script File 54
Upgrade Script File 54
Settings File 55
Contents of the Settings File 56
The GROUP System Value 57

Chapter 7: Administering Telephone Options 59
Administering Options for the 9600 Series IP Telephones 59
VLAN Considerations 66
VLAN Default Value and Priority Tagging 66
VLAN Separation. 67
DNS Addressing 68
IEEE 802.1X 69
802.1X Pass-Through and Proxy Logoff 69
802.1X Supplicant Operation 70
Local Administrative Options Using the Telephone Dialpad 71
Language Selection 72
Gigabit Ethernet Adapter 74
Enhanced Local Dialing 74
Backup/Restore 76
Backup 77
Restore 78

Chapter 8: Administering Applications and Options 81
Customizing 9600 Series IP Telephone Applications and Options. 81
The Application Status Flag (APPSTAT) 84

Appendix A: Glossary of Terms 87

Appendix B: Related Documentation 89
IETF Documents 89
ITU Documents. 90
ISO/IEC, ANSI/IEEE Documents 91

Index 93

Chapter 1: Introduction

About This Guide

This guide is for personnel who administer Avaya Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP Telephones, a Local Area Network (LAN), or a Web server.

The 9600 Series IP Telephones use Internet Protocol (IP) technology with Ethernet line interfaces and support the H.323 protocol only. The 9600 Series IP Telephones provide support for DHCP, HTTP, and HTTPS over IPv4/UDP, which enhance the administration and servicing of the telephones. These telephones use DHCP to obtain dynamic IP Addresses, and HTTPS or HTTP to download new versions of software or customized settings for the telephones.

Note:

Unless otherwise indicated, any reference to "the DEFINITY® server" in this document also refers to Avaya Communication Manager media servers.

CAUTION:

Avaya does not support many of the products mentioned in this document. Take care to ensure that there is adequate technical support available for servers used with any 9600 Series IP Telephone system. If the servers are not functioning correctly, the 9600 Series IP Telephones might not operate correctly.

Tip:

For a quick reference to Avaya Communication Manager settings for 9600 Series IP Telephones and related telephone interface information, see *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Read This First* (Document Number 16-601533), available at: www.avaya.com/support.

Differences Between 9600 Series and 4600 Series IP Telephones

Review this section if you administer both 4600 and 9600 Series IP Telephones.

Signaling - 46xx Series IP Telephones can use H.323 or SIP for telephony signaling. 96xx Series IP Telephones only use H.323. SIP-related administration of 96xx telephones is neither necessary nor relevant.

Avaya Communication Manager Release - 46xx telephones are supported prior to Communication Manager Release 3.0. The 96xx telephones are not officially supported prior to Release 3.0.

DHCP & SSON - 46xx telephones use Option 176 as the default DHCP Site Specific Option Number (SSON); 96xx telephones use Option 242.

Upgrade Script - The upgrade script files have different names and content (“46xxupgrade.scr” versus “96xxupgrade.txt”).

File Servers - 46xx telephones can use either TFTP or HTTP servers as file servers, for example, to download new phone firmware, upgrade script files, or settings files. 96xx telephones only use HTTP.

Backup - 46xx telephones use FTP as the protocol to create and access backup files. Users can specify unique backup server addresses, backup directories, FTP User IDs, and FTP User Passwords. 96xx telephones use HTTP as the protocol to create and access backup files, and users have no options to change backup parameters. 96xx telephones use the settings file parameter BRURI to identify the backup file site.

Backup Filenames - 96xx telephones store their backup files with titles that do not include the model number, for example, ***1234_96xxdata.txt*** vs. ***1234_4610data.txt*** or ***1234_4620data.txt***.

Backup File Content - Backup file contents are generally the same, except that the 96xx Contacts data is stored as:

ABKNAME*mmm* = label
ABKNUMBER*mmm* = telephone number
ABKTYPE*mmm* = entry type

where ***mmm*** is **001** to **250**. A given Contact entry in the 96xx Backup file must have both name and number to be valid. Type is optional and not applicable for Releases 1.0 and 1.1. **ABK** stands for “Address Book”, the original Contacts application name.

Settings File - Although both 46xx and 96xx telephones use the 46xxsettings file, the 96xx uses the following new parameters:

BRURI - to specify a URI to place the backup file
HTTPDIR - to specify a subdirectory path on the HTTP server
MSGNUM - for voice mail access
UNNAMEDSTAT - to turn Unnamed Registration off/on

Any 46xx telephone receiving these 96xx-specific parameters ignores them.

IR/SMTP - 96xx telephones do not support Infrared (IR) or Simple Message Transport Protocol (SMTP), so any such 46xx administration is ignored.

Local Administration - The 46xx QOS, CTI, and ALERT Local Procedures are not supported by the 96xx telephones. Also, there is no indication of IR interfaces in the INT Local Procedure.

Language - As of Release 1.1, 96xx IP Telephones allow language administration.

SNMP & MIBs - Although both 46xx and 96xx telephones support SNMP v2c and have custom Management Information Bases (MIBs), the MIBs are formatted somewhat differently. Note that as of Release 1.1, SNMP is disabled by default in both IP Telephone series. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING system values appropriately.

Wideband Codecs - 96xx telephones support G.722 (wide band) codecs, unlike 46xx telephones.

Feature Button Administration - Although 96xx telephones do not require administration of the following feature buttons, the user experience is enhanced if they are administered: Conference Display, Selective Conference Party Mute, Send All Calls (SAC).

Issue Date

This document was issued for the first time in July, 2006 and updated for Release 1.1 in September, 2006.

What’s New in Release 1.1

The primary emphasis of Release 1.1 is to provide multiple language capability on a telephone by telephone basis. Three new system parameters let administrators customize the language in which the telephone displays text, and let users choose a language from up to four different languages:

- LANG0STAT,
- LANGxFILE, and
- LANGSYS

For more information, see Language Selection on page 72. The *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* describes a new local administrative procedure, MLS (Multiple Language Strings) to view language strings.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this document.
Chapter 2: Administration Overview and Requirements	Provides an overview of the administrative process and describes general hardware, software, and operational requirements.
Chapter 3: Network Requirements	Describes administrative requirements for your Local Area Network.
Chapter 4: Communication Manager Administration	Describes how to administer Avaya Communication Manager to operate with 9600 Series IP Telephones.
Chapter 5: Server Administration	Describes DHCP, TFTP, and HTTP administration for the 9600 Series IP Telephones.
Chapter 6: Telephone Software and Application Files	Describes telephone software, covers application software downloads, and provides information about the configuration file.
Chapter 7: Administering Telephone Options	Describes how to use file parameters and options to administer 9600 Series IP Telephones. Covers backup and restoration of telephone data. Also describes how to use local procedures to customize a single telephone from the dialpad.
Chapter 8: Administering Applications and Options	Provides a table of customizable application-specific parameters, to provide administrative control of telephone functions and options.
Appendix A: Glossary of Terms	Provides a glossary of terms used in this document or which can be applicable to 9600 Series IP Telephones.
Appendix B: Related Documentation	Provides references to external documents that relate to telephony in general, which can provide additional information about specific aspects of the telephones.

Other Documentation

See the Avaya support site at http://www.avaya.com/support for 9600 Series IP Telephone technical and end user documentation.

See Appendix B: Related Documentation for a list of non-Avaya documents, such as those published by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU).

Chapter 2: Administration Overview and Requirements

9600 Series IP Telephones

The 9600 Series IP Telephones currently support the H.323 signaling protocol.

The H.323 standard provides for real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling,
- H.245 for control signaling,
- Real Time Transfer Protocol (RTP), and
- Real Time Control Protocol (RTCP)

The parameters under which the 9600 Series IP Telephones need to operate are summarized as follows:

- Telephone Administration on the Avaya Media Server, as covered in Chapter 4: Communication Manager Administration.
- IP address management for the telephone, as covered in DHCP and File Servers on page 35 for dynamic addressing. For static addressing, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.
- Tagging Control and VLAN administration for the telephone, if appropriate, as covered in Chapter 7: Administering Telephone Options.
- Quality of Service (QoS) administration for the telephone, if appropriate. QoS is covered in QoS on page 23 and QoS on page 31.
- Interface administration for the telephone, as appropriate. Administer the telephone to LAN interface using the PHY1 parameter described in Chapter 3: Network Requirements. Administer the telephone to PC interface using the PHY2 parameter described in “Local Procedures” in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide.*
- Application-specific telephone administration, if appropriate, as described in Chapter 8: Administering Applications and Options. An example of application-specific data is Web-specific information required for this optional application.

Table 1 indicates that you can administer system parameters in a variety of ways and use a variety of delivery mechanisms like:

- Maintaining the information on the call server.
- Manually entering the information by means of the telephone dialpad.
- Administering the DHCP server.
- Editing the configuration file on the applicable HTTP or HTTPS file server.
- User modification of certain parameters, when given administrative permission to do so.

Note:

Not all parameters can be administered on all delivery mechanisms.

Table 1: Administration Alternatives and Options for 9600 Series IP Telephones

Parameter(s)	Administrative Mechanisms	For More Information See:
Telephone Administration	Avaya call server	Chapter 4: Communication Manager Administration, Chapter 5: Server Administration, and Appendix B: Related Documentation.
IP Addresses	DHCP (strongly recommended)	DHCP and File Servers on page 35, and especially DHCP Server Administration on page 36.
	Configuration file	Chapter 6: Telephone Software and Application Files and Chapter 7: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
Tagging and VLAN	DHCP	DHCP Server Administration on page 36, and Chapter 7: Administering Telephone Options.
	Configuration file (strongly recommended)	DHCP and File Servers on page 35 and Chapter 7: Administering Telephone Options.
	Manual administration at the telephone	"Static Addressing Installation" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

1 of 2

Table 1: Administration Alternatives and Options for 9600 Series IP Telephones (continued)

Parameter(s)	Administrative Mechanisms	For More Information See:
Quality of Service	Avaya call server (strongly recommended)	UDP Port Selection on page 30 and Appendix B: Related Documentation.
	DHCP	DHCP and File Servers on page 35, and Chapter 7: Administering Telephone Options.
	Configuration file	DHCP and File Servers on page 35, and Chapter 7: Administering Telephone Options.
Interface	DHCP	DHCP and File Servers on page 35, and Chapter 6: Telephone Software and Application Files.
	Configuration file (strongly recommended)	DHCP and File Servers on page 35, and Chapter 6: Telephone Software and Application Files.
	Manual administration at the telephone	"Secondary Ethernet (Hub) Interface Enable/ Disable" in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
Application - specific parameters	DHCP	DHCP and File Servers on page 35, and especially DHCP Server Administration on page 36. Also, Chapter 8: Administering Applications and Options.
	Configuration file (strongly recommended)	DHCP and File Servers on page 35, and especially HTTP Generic Setup on page 47. Also, Chapter 8: Administering Applications and Options.

2 of 2

General information about administering DHCP servers is covered in DHCP and File Servers on page 35, and more specifically, DHCP Server Administration on page 36. General information about administering HTTP servers is covered in DHCP and File Servers, and more specifically, HTTP Generic Setup. Once you are familiar with that material, you can administer telephone options as described in Chapter 7: Administering Telephone Options.

Parameter Data Precedence

If a given parameter is administered in multiple places, the last server to provide the parameter has precedence. The precedence, from lowest to highest, is:

1. Manual administration, with the two exceptions described for the system parameter STATIC on page 64,
2. DHCP,
3. HTTP,
4. the Avaya Media Server, and finally,
5. Backup files, if administered and if permitted.

Settings the IP telephone receives from backup files or the media server overwrite any previous settings, including manual settings. The only exception to this sequence is in the case of VLAN IDs. In the case of VLAN IDs, the usual sequence applies through HTTP. If the VLAN ID after HTTP is not zero, any VLAN ID from the media server is ignored.

The Administrative Process

The following list depicts administration for a typical 9600 Series IP Telephone network. Your own configuration might differ depending on the servers and system you have in place.

1. Switch administered for 9600 Series IP Telephones.
2. LAN and applicable servers administered to accept the telephones.
3. Telephone software downloaded from the Avaya support site.
4. 46xxsettings file updated with site-specific information, as applicable.
5. 9600 Series Telephones installed. For more information, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
6. Individual 9600 Series IP Telephones updated using local procedures, as applicable. For more information, see “Local Administrative Procedures” in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Administrative Checklist

Use the following checklist as a guide to system and LAN administrator responsibilities. This high-level list helps ensure that all telephone system prerequisites and requirements are met prior to telephone installation.

Note:

One person might function as both the system administrator and the LAN administrator in some environments.

Table 2: Administrative Checklist

Task	Description	For More Information See:
Network Requirements Assessment	Determine that network hardware is in place and can handle telephone system requirements.	Chapter 3: Network Requirements.
Administer the call server	Verify that the call server is licensed and is administered for Voice over IP (VoIP). Verify the individual telephones are administered as desired.	Chapter 4: Communication Manager Administration. Chapter 4: Communication Manager Administration.
DHCP server installation	Install a DHCP application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Administer DHCP application	Add IP telephone administration to DHCP application.	DHCP Server Administration in Chapter 5: Server Administration.
HTTP/HTTPS server installation	Install an HTTP/HTTPS application on at least one new or existing PC on the LAN.	Vendor-provided instructions.
Application file(s), script file, and settings file installation on HTTP/ HTTPS server	Download the files from the Avaya support site.	http://www.avaya.com/support Chapter 6: Telephone Software and Application Files.
Modify settings file as desired	Edit the settings file as desired, using your own tools or the [Avaya] Web configuration tool.	Chapter 6: Telephone Software and Application Files and Web Configuration Tool on page 50.

1 of 2

Table 2: Administrative Checklist (continued)

Task	Description	For More Information See:
Administer WML servers	Add WML content as applicable to new or existing WML servers. Administer push content as applicable.	*Avaya one-X™Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-600888).
Administer telephones locally as applicable	As a Group:	The GROUP System Value on page 57 and the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
	Individually:	The applicable Local Procedures in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.*
Installation of telephones in the network		*Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.
Allow user to modify Options, if applicable		OPSTAT on page 62 and the respective User Guide for the specific telephone model.

2 of 2

Telephone Initialization Process

These steps offer a high-level description of the information exchanged when the telephone initializes and registers. This description assumes that all equipment is properly administered ahead of time. This description can help you understand how the 9600 Series IP Telephones relate to the routers and servers in your network.

Step 1: Telephone to Network

The telephone is appropriately installed and powered. After a short initialization process, the telephone identifies the LAN speed and sends a message out into the network, identifying itself and requesting further information. A router on the network receives and relays this message to the appropriate DHCP server.

Step 2: DHCP Server to Telephone

The DHCP file server provides information to the telephone, as described in DHCP and File Servers on page 35. Among other data passed to the telephone is the IP address of the HTTP or HTTPS server.

Step 3: Telephone and File Server

The 9600 Series IP Telephones can download script files, application files, and settings files from either an HTTP or HTTPS server. The telephone queries the file server, which transmits a script file to the telephone. This script file, at a minimum, tells the telephone which application file the telephone must use. The application file is the software that has the telephony functionality.

The telephone uses the script file to determine if it has the proper application file. If the telephone determines the proper application file is missing, the telephone requests an application file download from the file server. The file server then downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds as described in the next paragraph without downloading the application file again.

The telephone checks and loads the application file, then uses the script file to look for a settings file, if appropriate. The optional settings file can contain settings you have administered for any or all of the 9600 Series IP Telephones in your network. For more information about this download process and settings file, see Chapter 6: Telephone Software and Application Files.

Step 4: Telephone and the Call Server

The call server referred to in this step is the Avaya Media Server.

In this step, the telephone might prompt the user for an extension and password. The telephone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the telephone extension and the call server password. For a restart of an existing installation, this information is already stored on the telephone, but the user might have to confirm the information. The telephone and the call server exchange more messaging. The expected result is that the telephone is appropriately registered and call server data such as feature button assignments are downloaded.

The 9600 Series IP Telephones support a feature called Unnamed Registration. Unnamed Registration allows a telephone to register with the Avaya Media Server without an extension, assuming the Avaya Media Server also supports this feature. To invoke Unnamed Registration, take no action. Allow the **Extension...** prompt display for 60 seconds without making an entry. The telephone automatically attempts to register by means of Unnamed Registration. A telephone registered with Unnamed Registration has the following characteristics:

- only one call appearance,
- no administrable features,
- can make only outgoing calls, subject to call server Class of Restriction/Class of Service limitations, and
- can be converted to normal “named” registration by the user entering a valid extension and password.

You can also administer the telephone to avoid unnamed registration and remain unregistered if no extension and password are provided. For more information, see UNNAMEDSTAT in Table 7.

For more information about the installation process, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Error Conditions

Assuming proper administration, most of the problems reported by telephone users are likely to be LAN-based. Quality of Service, server administration, and other issues can impact user perception of IP telephone performance.

The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* covers possible operational problems that might be encountered after successful 9600 Series IP Telephone installation. The following User Guides also contain guidance for users having problems with specific IP telephone applications:

- *Avaya one-X™ Deskphone Edition for 9620 IP Telephone User Guide*
- *Avaya one-X™ Deskphone Edition for 9630 IP Telephone User Guide*

Chapter 3: Network Requirements

Network Assessment

Perform a network assessment to ensure that the network will have the capacity for the expected data and voice traffic, and that it can support for all applications:

- H.323,
- DHCP,
- HTTP/HTTPS, and
- Jitter buffers

Also, QoS support is required to run VoIP on your configuration. For more information, see Appendix B: Related Documentation and UDP Port Selection on page 30.

Hardware Requirements

To operate properly, you need:

- Category 5e cables designed to the IEEE 802.3af-2003 standard, for LAN powering,
- TN2602 IP Media Processor circuit pack. Sites with a TN2302 IP Media Processor circuit pack must also install a TN2602 circuit pack.
- TN799C or D Control-LAN (CLAN) circuit pack.

Important:

IP telephone firmware Release 1.0 or greater requires TN799C V3 or greater CLAN circuit pack(s). For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support Web site http://www.avaya.com/support.

To ensure that the appropriate circuit pack(s) are administered on your media server, see Chapter 4: Communication Manager Administration. For more information about hardware requirements in general, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Server Requirements

Three server types can be configured for the 9600 Series IP Telephones:

- DHCP
- HTTP or HTTPS
- Web (optional)

While the servers listed provide different functions that relate to the 9600 Series IP Telephones, they are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can co-exist on one hardware unit. Any standards-based server is recommended.

For parameters related to Avaya Media Server information, see Chapter 4: Communication Manager Administration, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Chapter 5: Server Administration.

CAUTION:

The telephones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the DHCP file server is unavailable when the telephones reset, the telephones register with the media server and operate. Some features might not be available. To restore them you need to reset the telephone(s) when the file server is available.

DHCP Server

Avaya recommends that a DHCP server and application be installed and that static addressing be avoided. Install the DHCP server and application as described in DHCP and File Servers on page 35.

HTTP/HTTPS Server

Administer the HTTP or HTTPS file server and application as described in HTTP Generic Setup on page 47.

Web Server (Optional)

If users are to have access to corporate WML Web sites, administer the telephones as described in Chapter 5: Server Administration.

For routine WML functionality only a WML server is required. For “push” functionality, a Trusted Push Server is needed. The Trusted Push Server can be the same server as your routine WML server. Separate the two functions for security purposes. Avaya recommends that you restrict access to push directories on the WML server.

Your Web server configuration must be compatible with the requirements covered in the *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

Required Network Information

Before you administer DHCP and HTTP, and TLS, as applicable, complete the information in Table 3. If you have more than one Gateway, HTTP/TLS server, subnetwork mask, and Gatekeeper in your configuration, complete Table 3 for each DHCP server.

The 9600 Series IP Telephones support specifying a list of IP addresses for a gateway/router, HTTP/HTTPS server, and Avaya Media Server Gatekeeper(s). Each list can contain up to 255 total ASCII characters, with IP addresses separated by commas with no intervening spaces. Depending on the specific DHCP application, only 127 characters might be supported.

When specifying IP addresses for the file server or media server, use either dotted decimal format (“xxx.xxx.xxx.xxx”) or DNS names. If you use DNS, the system value DOMAIN is appended to the IP addresses you specify. If DOMAIN is null, the DNS names must be fully qualified, in accordance with IETF RFCs 1034 and 1035. For more information about DNS, see DHCP Generic Setup on page 36 and DNS Addressing on page 68.

Table 3: Required Network Information Before Installation - Per DHCP Server

1. Gateway (router) IP address(es)	
2. HTTP server IP address(es)	
3. Subnetwork mask	
4. Avaya Media Server Gatekeeper IP address(es)	
5. Avaya Media Server Gatekeeper port	Although this can be a value between 0 and 65535, the default value is **1719**. Do not change the default value unless that value conflicts with an existing port assignment.
6. HTTP server file path	
7. Telephone IP address range *From*: *To*:	
8. DNS server address(es)	If applicable.
9. HTTPS server address(es)	If applicable.

The file server file path is the “root” directory used for all transfers by the server. All files are uploaded to or downloaded from this default directory. In configurations where the upgrade script and application files are in the default directory, do not use item 6 in Table 3.

As the LAN or System Administrator, you are also responsible for:

- Administering the DHCP server as described in Chapter 5: Server Administration.
- Editing the configuration file on the applicable HTTP or HTTPS file server, as covered in 9600 Series IP Telephone Scripts and Application Files.

Other Network Considerations

SNMP

The 9600 Series IP Telephones are fully compatible with SNMPv2c and with Structure of Management Information Version 2 (SMIv2). The telephones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. “Fully compatible” means that the telephones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that the values therein cannot be changed externally by means of network management tools.

You can restrict which IP addresses the telephone accepts SNMP queries from. You can also customize your community string with system values SNMPADD and SNMPSTRING, respectively. For more information, see Chapter 5: Server Administration and Table 7: 9600 Series IP Telephone Customizable System Parameters.

Note:

As of Release 1.1, SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING system values appropriately.

For more information about SNMP and MIBs, see the IETF references listed in Appendix B: Related Documentation. The Avaya Custom MIB for the 9600 Series IP Telephones is available for download in *.txt format on the Avaya support Web site at http://www.avaya.com/support.

Reliability and Performance

All 9600 Series IP Telephones respond to a ping or traceroute message sent from the DEFINITY®, MultiVantage™, or Avaya Communication Manager switch or any other network source. The telephones do not originate a ping or traceroute. The 9600 Series IP Telephones offer and support “remote ping” and “remote traceroute.” The switch can instruct the telephone to originate a ping or a traceroute to a specified IP address. The telephone carries out that instruction and sends a message to the switch indicating the results. For more information, see your switch administration documentation.

If applicable, the telephones test whether the network Ethernet switch port supports IEEE 802.1D/q tagged frames by ARPing the router with a tagged frame. For more information, see VLAN Considerations on page 66. If your LAN environment includes Virtual LANs (VLANs), your router must respond to ARPs for VLAN tagging to work properly.

QoS

For more information about the extent to which your network can support any or all of the QoS initiatives, see your LAN equipment documentation. See QoS on page 31 about QoS implications for the 9600 Series IP Telephones.

All 9600 Series IP Telephones provide some detail about network audio quality. For more information see, Network Audio Quality Display on 9600 Series IP Telephones on page 24.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series IP Telephones, see IEEE 802.1D and 802.1Q on page 31 and VLAN Considerations on page 66. Three bits of the 802.1Q tag are reserved for identifying packet priority to allow any one of eight priorities to be assigned to a specific packet.

- **7:** Network management traffic
- **6:** Voice traffic with less than 10ms latency
- **5:** Voice traffic with less than 100ms latency
- **4:** “Controlled-load” traffic for critical data applications
- **3:** Traffic meriting “extra-effort” by the network for prompt delivery, for example, executive e-mail
- **2:** Reserved for future use
- **0:** The default priority for traffic meriting the “best-effort” for prompt delivery of the network.
- **1:** Background traffic such as bulk data transfers and backups

Note:

Priority 0 is a higher priority than Priority 1.

Network Audio Quality Display on 9600 Series IP Telephones

All 9600 Series IP Telephones give the user an opportunity to monitor network audio performance while on a call. For more information, see the telephone user guide.

While on a call, the telephones display network audio quality parameters in real-time, as shown in Table 4:

Table 4: Parameters in Real-Time

Parameter	Possible Values
Received Audio Coding	***G.711***, ***G.722***, ***G.726A***, or ***G.729***.
Packet Loss	No data or a percentage. Late and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any potential delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is one-half the value RTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay introduced by the jitter buffer of the telephone.

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

IP Address Lists and Station Number Portability

The 9600 Series IP Telephones provide the capability to specify IP address lists. On startup or a reboot, the telephone attempts to establish communication with these various network elements in turn. The telephone starts with the first address on the respective list. If the communication is denied or times out, the telephone proceeds to the next address on the appropriate list and tries that one. The telephone does not report failure unless all the addresses on a given list fail, thereby improving the reliability of IP telephony.

This capability also has the advantage of making station number portability easier. Assume a situation where the company has multiple locations in London and New York, all sharing a corporate IP network. Users want to take their telephones from their offices in London and bring them to New York. When users start up their telephones in the new location, the local DHCP server usually routes them to the local call server. With proper administration of the local DHCP server, the telephone knows to try a second call server IP address, this one in London. The user can then be automatically registered with the London call server.

Chapter 5: Server Administration contains details on administration of DHCP servers for lists of alternate media servers, router/gateways, and HTTP/HTTPS servers. For more information, see DNS Addressing on page 68.

TCP/UDP Port Utilization

The 9600 Series IP Telephones use a variety of protocols, particularly TCP and UDP, to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. For additional TCP/UDP port utilization information as it applies to Avaya Communication Manager, see UDP Port Selection on page 30.

Depending on your network, you might need to know what ports or ranges are used in the operation of 9600 Series IP Telephones. Knowing these ports or ranges helps you administer your networking infrastructure.

In Figure 1, Figure 2, and Figure 3:

- The box on the left always represents the 9600 Series IP Telephone.
- Depending on the diagram, the boxes on the right refer to various pieces of network equipment with which the telephone can communicate.
- Open-headed arrows (for example,) represent the direction(s) of socket initialization.
- Closed-headed arrows (for example,) represent the direction(s) of data transfer.
- The text the arrows point to identifies the port or ports that the 9600 Series IP Telephones support for the specific situation. Brackets identify ranges when more than one port applies. The text indicates any additional qualifications or clarifications. In many cases, the ports used are the ones called for by IETF or other standards bodies.
- Many of the explanations in the diagrams refer to system parameters or options settings, for example, DIRSRVR. For more information about parameters and settings, see Administering Options for the 9600 Series IP Telephones.

Figure 1: Signaling, Audio and Management Diagram

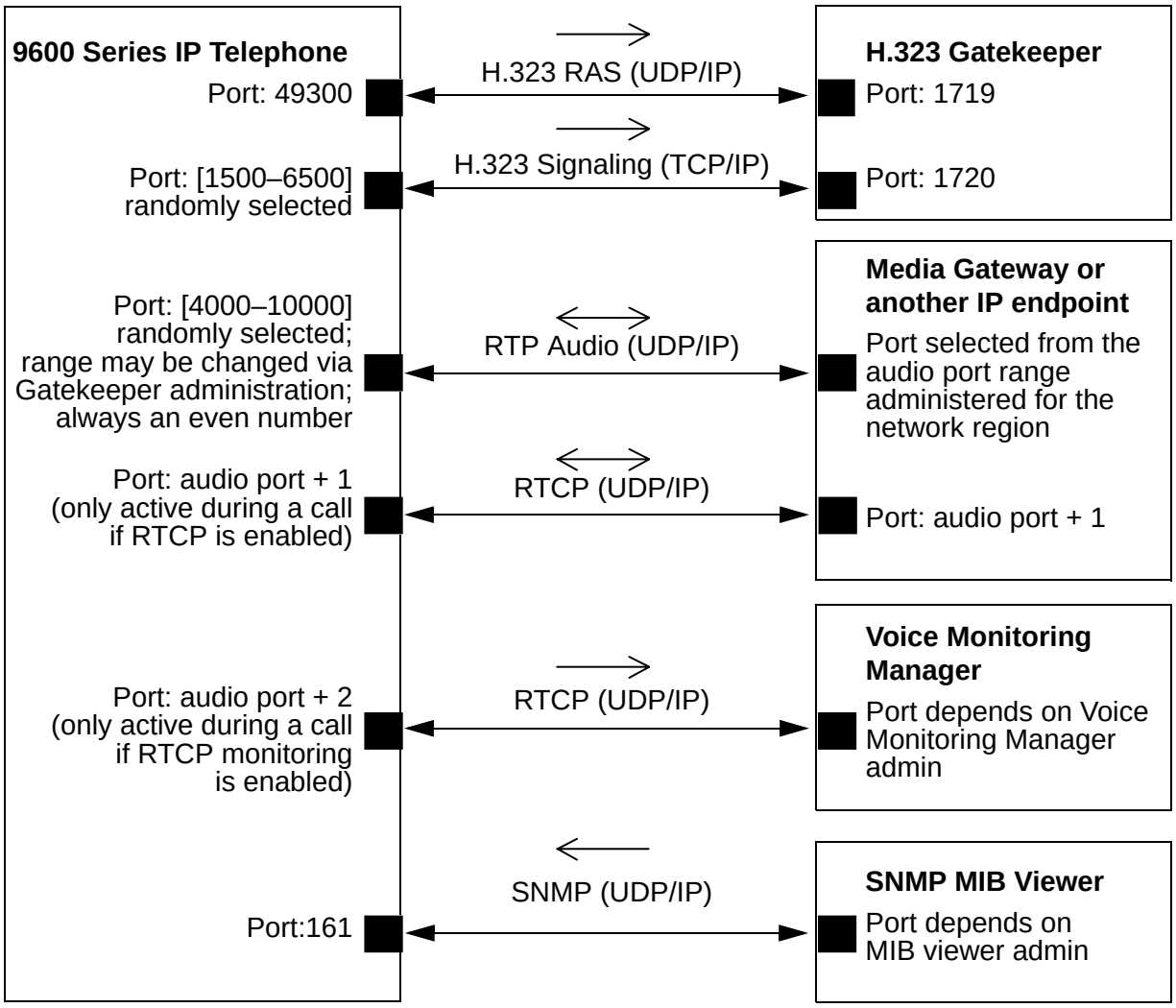

Signaling, Audio and Management
9600 Series IP Telephone
Port: 49300
Port: [1500–6500] randomly selected
Port: [4000–10000] randomly selected; range may be changed via Gatekeeper administration; always an even number
Port: audio port + 1 (only active during a call if RTCP is enabled)
Port: audio port + 2 (only active during a call if RTCP monitoring is enabled)
Port:161
H.323 RAS (UDP/IP)
H.323 Signaling (TCP/IP)
RTP Audio (UDP/IP)
RTCP (UDP/IP)
RTCP (UDP/IP)
SNMP (UDP/IP)
H.323 Gatekeeper
Port: 1719
Port: 1720
Media Gateway or another IP endpoint
Port selected from the audio port range administered for the network region
Port: audio port + 1
Voice Monitoring Manager
Port depends on Voice Monitoring Manager admin
SNMP MIB Viewer
Port depends on MIB viewer admin

Figure 2: Initialization and Address Resolution Diagram

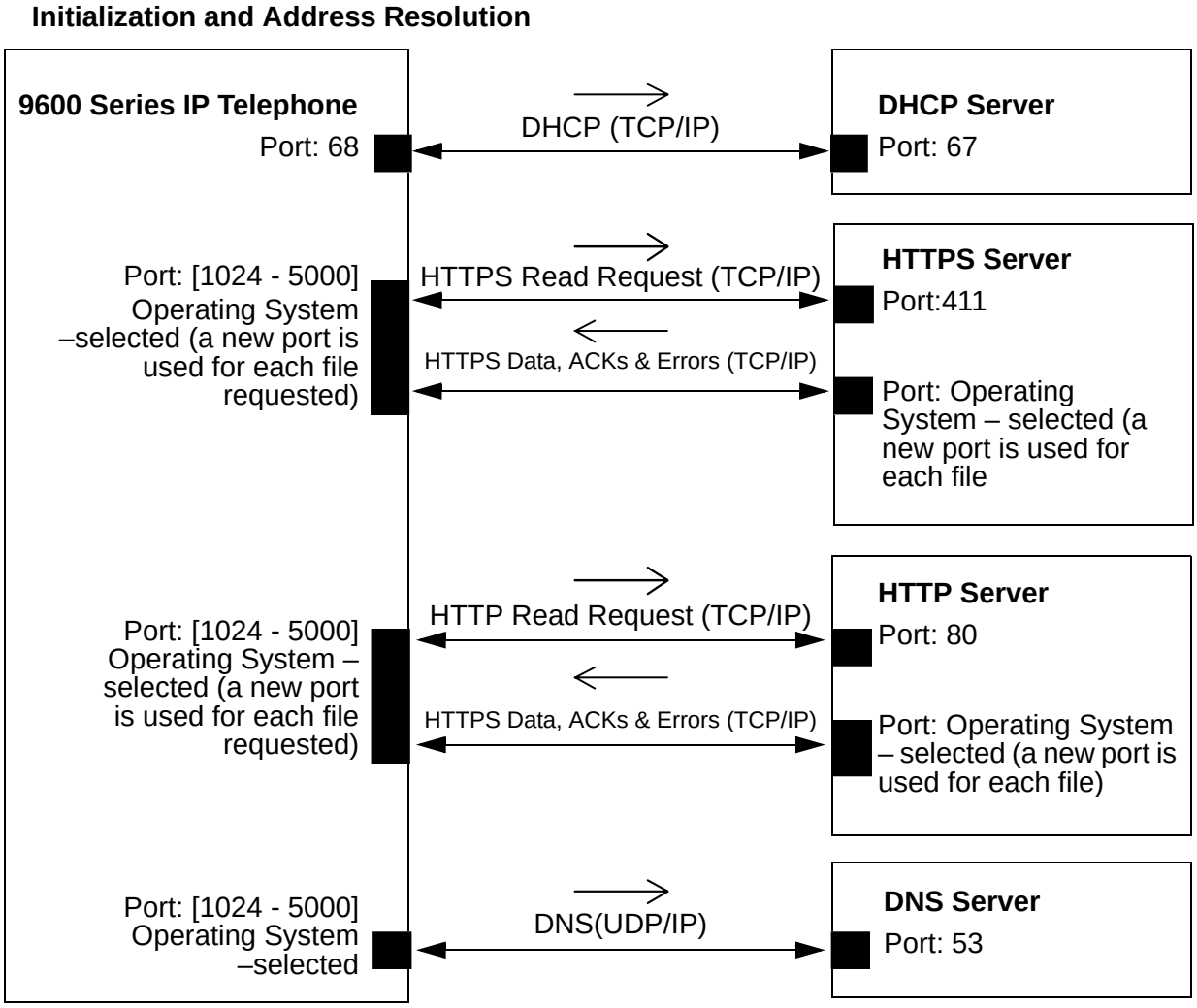
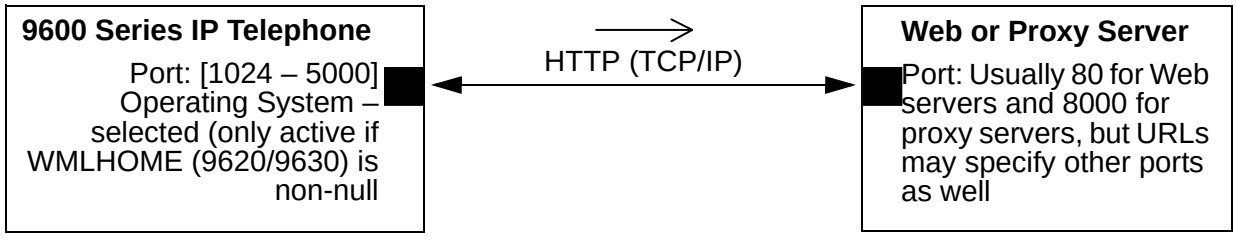

Initialization and Address Resolution
9600 Series IP Telephone
Port: 68
DHCP (TCP/IP)
DHCP Server
Port: 67
Port: [1024 - 5000] Operating System –selected (a new port is used for each file requested)
HTTPS Read Request (TCP/IP)
HTTPS Server
Port:411
HTTPS Data, ACKs & Errors (TCP/IP)
Port: Operating System – selected (a new port is used for each file
Port: [1024 - 5000] Operating System – selected (a new port is used for each file requested)
HTTP Read Request (TCP/IP)
HTTP Server
Port: 80
HTTPS Data, ACKs & Errors (TCP/IP)
Port: Operating System – selected (a new port is used for each file)
Port: [1024 - 5000] Operating System –selected
DNS(UDP/IP)
DNS Server
Port: 53

Figure 3: Applications Diagram


Applications
9600 Series IP Telephone
Port: [1024 – 5000] Operating System – selected (only active if WMLHOME (9620/9630) is non-null
HTTP (TCP/IP)
Web or Proxy Server
Port: Usually 80 for Web servers and 8000 for proxy servers, but URLs may specify other ports as well

Security

For information about toll fraud, see the DEFINITY® or Avaya Communication Manager documents on the Avaya support Web site. The 9600 Series IP Telephones cannot guarantee resistance to all Denial of Service attacks. However, there are checks and protections to resist such attacks while maintaining appropriate service to legitimate users.

All 9600 Series IP Telephones that have WML Web applications support Transport Layer Security (TLS). This standard allows the telephone to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. This setup adds security over another alternative.

You also have a variety of optional capabilities to restrict or remove how crucial network information is displayed or used. These capabilities are covered in more detail in Chapter 5: Server Administration.

- Support signaling channel encryption while registering, and when registered, with appropriately administered Avaya Media Servers.

  Note:

  Signaling and audio are not encrypted when unnamed registration is effective.

- Restricting the response of the 9600 Series IP Telephones to SNMP queries to only IP addresses on a list you specify.
- Specifying an SNMP community string for all SNMP messages the telephone sends.
- Restricting dialpad access to Local Administration Procedures, such as specifying IP addresses, with a password.
- Removing dialpad access to most Local Administration Procedures.
- Restricting the end user's ability to use a telephone Options application to view network data.

Registration and Authentication

The Avaya Media Server supports using the extension and password to register and authenticate 9600 Series IP Telephones. For more information, see the current version of your call server administration manual.

Chapter 4: Communication Manager Administration

Call Server Requirements

Before you perform administration tasks, ensure that the proper hardware is in place, and your call server software is compatible with the 9600 Series IP Telephones. Avaya recommends the latest PBX software and the latest IP telephone firmware.

Switch Compatibility and Aliasing IP Telephones

If you have Avaya Communication Manager (CM) Release 3.1 or earlier you must alias the telephones as follows:

9600 Series Telephone Model	Aliased as...	Earliest CM Release
9620	4610SW (recommended)	Avaya Communication Manager 3.0
	4620SW	Avaya Communication Manager 3.0
9630	4620SW	Avaya Communication Manager 3.0

Note:

Although support for a 9620 aliased as a 4620SW IP Telephone extends back to DEFINITY Release 11, some features are not available. For example, the 9620 only supports a total of 12 call appearances and administered feature buttons. The 4620 can be administered for a total of 24 call appearances and feature buttons.

For more information about aliasing one telephone model as another, see “Using an Alias” in the *Administrator Guide for Avaya Communication Manager* (Document 03-300509).

Media Server (Switch) Administration

For information about specific switch administration, see the following documents on the Avaya support Web site:

- The *Administrator Guide for Avaya Communication Manager* (Document 03-300509) provides detailed instructions for administering an IP telephone system on Avaya Communication Manager. See Chapter 3 “Managing Telephones,” which describes the process of adding new telephones. Also, you can locate pertinent screen illustrations and field descriptions in Chapter 19 “Screen References” of that guide.
- *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) provides detailed information about switch administration for your network.

IP Interface and Addresses

Follow these general guidelines:

- Define the IP interfaces for each CLAN and Media processor circuit pack on the switch that uses the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document 555-233-504).
- On the Customer Options form, verify that the **IP Stations** field is set to “**y**” (Yes). If it is not, contact your Avaya sales representative. The **IP Softphone** field does not have to be set to “**y**” (Yes).

UDP Port Selection

The 9600 Series IP Telephones can be administered from the Avaya Communication Manager Network Region form to support UDP port selection. Locate specific port assignment diagrams in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*. For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) on the Avaya support Web site.

Administer the switch to use a port within the proper range for the specific LAN, and the IP telephone(s) copy that port. If no UDP port range is administered on the switch, the IP telephone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

RSVP and RTCP

Avaya IP Telephones implement the Resource ReSerVation Protocol (RSVP) administered from the media server and the RTP Control Protocol (RTCP). The Avaya Voice over IP (VoIP) Monitoring Manager (VMON) software can then provide real-time monitoring and historical data of audio quality for VoIP calls.

The only way to change these parameters is by appropriate switch administration. For more information, see your Avaya Media Server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager (*Document Number 555-233-504).

QoS

The 9600 Series IP Telephones support both IEEE 802.1D/Q and DiffServ. Other network-based QoS initiatives such as UDP port selection do not require support by the telephones. However, they contribute to improved QoS for the entire network.

IEEE 802.1D and 802.1Q

The 9600 Series IP Telephones can simultaneously support receipt of packets using, or not using, 802.1Q parameters. To support IEEE 802.1D/Q, you can administer 9600 Series IP Telephones from the network by appropriate administration of the DHCP or HTTP/HTTPS servers, or by using dialpad input at the telephone.

Important:

Avaya Communication Manager administration always takes precedence over manual administration of IEEE 802.1D/Q data.

The four IEEE 802.ID/Q QoS parameters in the telephones that can be administered on the IP Network Region form are **L2Q, L2QVLAN, L2QAUD, and L2QSIG.** To set these parameters at the switch, see “About Quality of Service (QoS) and voice quality administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). To set these parameters manually see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide.* You can specify VLAN ID and VLANTEST values with the ADDR Local Administrative Option.

Note:

All local administrative procedures are on a phone-by-phone basis. Administration using Communication Manager, DHCP, and HTTP applies to the telephone system itself or to a range of telephones.

NAT

Network Address Translation (NAT) usage can lead to problems that affect the consistency of addressing throughout your network. All H.323 IP Telephones support NAT interworking. Support for NAT does not imply support for Network Address Port Translation (NAPT). The telephones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the media server. A direct Avaya IP Telephone-to-Avaya IP Telephone call with NAT requires Avaya Communication Manager Release 3.0 or greater software. For more information, see *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504) on the Avaya support Web site.

DIFFSERV

The DiffServ values change to the values administered on the media server as soon as the telephone registers. For more information, see Chapter 4 “Network Quality Administration” in *Administration for Network Connectivity for Avaya Communication Manager* (Document Number 555-233-504). Unless there is a specific need in your enterprise LAN, Avaya recommends that you do not change the default values.

Voice Mail Integration

You can set the system parameter MSGNUM to any dialable string. An example is the telephone number users would dial to access your voice mail system such as AUDIX or Octel. For more information, see Table 7. When the user presses the Message button on the telephone, that number is automatically dialed, giving the user one-touch access to voice mail.

Call Transfer Considerations

This section provides information about call transfer behaviors to consider when administering the call server. The telephone application presents a user interface, based in part on the deduction of the call state. But, as the administrator, be aware that the following server-based features can interact with the user interface resulting in a call state that might need explanation:

- When the system parameter **Abort Transfer?** is set to *Yes*, once a transfer has been started the user cannot press a non-idle call appearance until the transfer is complete or the transfer is aborted.

- When the system parameter **Abort Transfer?** is set to *No*, the transfer proceeds normally even if the user presses a non-idle call appearance before the transfer is complete.
- When the system parameter **Transfer Upon Hang-up** is set to *No*, the user must press the **Complete** softkey after dialing the intended destination for the transfer to be completed.
- When the **Transfer Upon Hang-up** is set to *Yes*, the user can hang up immediately after dialing and the transfer proceeds normally.

The features **Abort Transfer** and **Transfer Upon Hang-up** can interact. If a user initiates a transfer, dials the destination, and hangs up without pressing the **Complete** softkey, the three possible outcomes are:

- The transfer is completed. This is the case when **Transfer Upon Hang-up** is set to *Yes*, regardless of the **Abort Transfer?** setting.
- The transfer is aborted. This is the case when **Transfer Upon Hang-up** is set to *No* and **Abort Transfer?** is set to *Yes*.
- The transfer is denied. This is the case when **Transfer Upon Hang-up** is set to *No* and **Abort Transfer?** is set to *No* and the call appearance of the transferee remains on soft hold.

Attempts to transfer an outside call to an outside line are denied. However, the user can drop the denied destination and initiate a transfer to an internal destination.

The call server feature, **Toggle Swap**, allows the user to swap the soft-held and setup call appearances. That is, the setup call appearance becomes soft-held, and the soft-held call appearance becomes active as the setup call appearance. This only works once the setup call appearance is connected on a call. If Toggle Swap is pressed while the setup call appearance has ringback, the call server sends a broken flutter to the setup call appearance. Toggle Swap is ignored without a broken flutter if pressed while the setup call appearance is still dialing. Toggle swapping the hold status of call appearances can be confusing to the user.

Conferencing Call Considerations

This section provides information about conference call behaviors to consider when administering the call server. The telephone application presents a user interface, based in part on the deduction of the call state. But, as the administrator, be aware that the following server-based features can interact with the user interface resulting in a call state that might need explanation:

- When the system parameter **Abort Conference Upon Hang-up** is set to *Yes*, the user must dial and press the **Complete** softkey for the conference to be completed. When the system parameter **Abort Conference Upon Hang-up** is set to *No*, the user can hang up immediately after dialing and the conference proceeds normally.

- When the system parameter **No Dial Tone Conferencing** is set to *No*, and the **Conference** or **Add** softkey is pressed, the call server automatically selects an idle call appearance for the user to dial on. This action allows the next conferee to be added. When the system parameter **No Dial Tone Conferencing** is set to *Yes*, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when **Select Line Conferencing** is set to *Yes*, which automatically sets **No Dial Tone Conferencing** to *Yes*. Specifically:

- If the user finishes dialing the intended conferee, pressing the initial call appearance allows the conference to proceed normally, as if the **Join** softkey was pressed.
- If the user has not finished dialing the intended conferee, pressing the initial call appearance (placed on soft hold when **Conference** or **Add** was pressed) cancels the conference set up.
- If the user presses the **Conference** or **Add** softkey, then immediately presses a hard-held call appearance, the previously held call appearance is retrieved from hold and joins the existing conference.

When the system parameter **Select Line Conferencing** is set to *No*, the user cancels the conference setup by pressing the call appearance on soft hold before pressing **Join**. Selecting a hard-held call appearance during conference setup establishes the held call as the intended conferee. If the user is in conference setup and answers an incoming call, the incoming call is established as the intended conferee, but **Join** must then be pressed. If the user does not want the incoming call to be part of the conference, the call should not be answered, or the call can be answered and then hung up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The **Toggle Swap** feature works for Conference setup just like it does for Transfer Setup. For more information, see the last paragraph of Call Transfer Considerations.

Telephone Administration

For detailed information about administering the media server for 9600 Series IP Telephones, see the following Avaya documents:

- *Administrator Guide for Avaya Communication Manager* (Document 03-300509).
- *Feature Description and Implementation for Avaya Communication Manager* (Document 555-245-770).

Other Considerations

When a 9620 IP Telephone is aliased as a 4620SW IP Telephone, do not administer:

- a button module (SBM24, EU24, or EU24BL), or
- feature buttons 13 through 24.

The 9630 IP Telephone can be administered for both of these options.

Chapter 5: Server Administration

Software Checklist

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

Note:

You can install the DHCP and HTTP server software on the same machine.

CAUTION:

The firmware in the 9600 Series IP Telephones reserves IP addresses of the form **192.168.2.x** for internal communications. The telephone(s) improperly use addresses you specify if they are of that form.

DHCP and File Servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for a 9600 Series IP Telephone network by removing the need to individually assign and maintain IP addresses and other parameters for each IP telephone on the network.

The DHCP server provides the following information to the 9600 Series IP Telephones:

- IP address of the 9600 Series IP Telephone(s)
- IP address of the Gatekeeper board on the Avaya Media Server
- IP address of the HTTP or HTTPS server
- The subnet mask
- IP address of the router
- DNS Server IP address

Administer the LAN so each IP telephone can access a DHCP server that contains the IP addresses and subnet mask.

The IP telephone cannot function without an IP address. The failure of a DHCP server at boot time leaves all the affected telephones unusable. A user can manually assign an IP address to an IP telephone. When the DHCP server finally returns, the telephone never looks for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Avaya recommends that:

- A minimum of two DHCP servers be available for reliability.
- A DHCP server be available when the IP telephone reboots.
- A DHCP server be available at remote sites if WAN failures isolate IP telephones from the central site DHCP server(s).

The file server provides the 9600 Series IP Telephone with a script file and, if appropriate, new or updated application software. See Step 3: Telephone and File Server on page 17 under Telephone Initialization Process. In addition, you can edit an associated settings file to customize telephone parameters for your specific environment. For more information, see Chapter 7: Administering Telephone Options.

DHCP Server Administration

This document concentrates on the simplest case of the single LAN segment. Information provided here can be used for more complex LAN configurations.

CAUTION:
Before you start, understand your current network configuration. An improper installation can cause network failures or reduce the reliability and performance of your network.

DHCP Generic Setup

This document is limited to describing a generic administration that works with the 9600 Series IP Telephones. Three DHCP software alternatives are common to Windows operating systems:

- Windows NT® 4.0 DHCP Server
- Windows 2000® DHCP Server
- Windows 2003® DHCP Server

Any other DHCP application might work. It is the responsibility of the customer to install and configure the DHCP server correctly.

DHCP server setup involves:

1. Installing the DHCP server software according to vendor instructions.
2. Configuring the DHCP server with:
   - IP addresses available for the 9600 Series IP Telephones.
   - The following DHCP options:
     - **Option 1 - Subnet mask**.
       As described in Table 3, item 3.
     - **Option 3 - Gateway (router) IP address(es)**.
       As described in Table 3, item 1. If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP addresses with commas with no intervening spaces.
     - **Option 6 - DNS server(s) address list**.
       If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
     - **Option 12 - Host Name**.
       Value is **AV*ohhhhhh***, where: *o* is “A” if the OID (first three octets) of the MAC address for the telephone is 00-04-0D. “E” if the OID is 00-09-6E, “L” if the OID is 00-60-1D, and “X” if the OID is anything else and where *hhhhhh* are ASCII characters for the hexadecimal representation of the last three octets of the MAC address for the telephone.
     - **Option 15 - DNS Domain Name**.
       This string contains the domain name to be used when DNS names in system parameters are resolved into IP addresses. This domain name is appended to the DNS name before the 9600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in DNS Addressing on page 68.
     - **Option 51 - DHCP lease time**.
       If this option is not received, the DHCPOFFER is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP Telephones to reboot. Avaya recommends providing enough leases so an IP address for an IP telephone does not change if it is briefly taken offline.

Note:

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given telephone. In this case the telephone is not usable until the server can be reached.
Avaya recommends, once assigned an IP address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. As Table 7: 9600 Series IP Telephone Customizable System Parameters indicates, the system parameter DHCPSTD allows an administrator to specify that the telephone will either:
a). Comply with the DHCP standard by setting DHCPSTD to “1”, or
b). Continue to use its IP address after the DHCP lease expires by setting DHCPSTD to “0.”

The latter case is the default. If the default is invoked, after the DHCP lease expires the telephone sends an ARP Request for its own IP address every five seconds.
The request continues either forever, or until the telephone receives an ARP Reply. After receiving an ARP Reply, the telephone displays an error message, sets its IP address to 0.0.0.0, and attempts to contact the DHCP server again.

- **Option 52 - Overload Option, if desired**.
  If this option is received in a message, the telephone interprets the **sname** and **file** fields in accordance with IETF RFC 2132,
  Section 9.3, listed in Appendix B: Related Documentation.
- **Option 53 - DHCP message type**.
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST).
- **Option 55 - Parameter Request List**.
  Acceptable values are:
  1 (subnet mask),
  3 (router IP address[es])
  6 (domain name server IP address[es])
  15 (domain name)
  NVSSON (site-specific option number)
- **Option 57 - Maximum DHCP message size**.
- **Option 58 - DHCP lease renew time**.
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5, listed in Related Documentation.
- **Option 59 - DHCP lease rebind time**.
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per RFC 2131, Section 4.5

The 9600 Series IP Telephones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for the 9600 Series IP Telephones on page 59.

In configurations where the upgrade script and application files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.

You do not have to use Option 242. If you do not use this option, you must ensure that the key information, especially HTTPSRVR and MCIPADD, is administered appropriately elsewhere.

Avaya recommends that you administer DHCP servers to deliver only the options specified in this document. Administering additional, unexpected options might have unexpected results, including causing the IP telephone to ignore the DHCP server.

The media server name and HTTP server name must each be no more than 32 characters in length.

Examples of good DNS administration include:

- Option 6: “***aaa.aaa.aaa.aaa***”
- Option 15: “***dnsexample.yourco.com,zzz.zzz.zzz.zzz***”
- Option 242: “**MCIPADD=*xxxx.xxx.xxx.xxx***”

Depending on the DHCP application you choose, be aware that the application most likely does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. For example, Windows NT® DHCP reserves expired leases for about one day. This reservation period protects a lease for a short time. If the client and the DHCP server are in two different time zones, the clocks of the computers are not in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period: Assume two IP addresses, therefore two possible DHCP leases. Assume three IP telephones, two of which are using the two available IP addresses. When the lease for the first two telephones expires, the third telephone cannot get a lease until the reservation period expires. Even if the other two telephones are removed from the network, the third telephone remains without a lease until the reservation period expires.

In Table 5, the 9600 Series IP Telephone sets the system values to the DHCPACK message field values shown.

Table 5: DHCPACK Setting of System Values

System Value	Set to
IPADD	The **yiaddr** field.
NETMASK	Option #1 (if received).
GIPADD	Option #3 (if received, which might be a list of IP addresses).
TLSSRVR	The **siaddr** field, if that field is non-zero.
HTTPSRVR	The **siaddr** field, if that field is non-zero.
DNSSRVR	Option #6 (if received, which might be a list of IP addresses).
DOMAIN	Option #15 (if received).
DHCP lease time	Option #51 (if received).
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).

Windows NT 4.0 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Settings**-->**Control Panel**.
2. Double-click the **Network** icon.
3. Verify that **Microsoft DHCP Server** is listed as one of the Network Services on the **Services** tab.
4. If it is listed, continue with the next section. If it is not listed, install the DHCP server.

Creating a DHCP Scope for the IP Telephones

Use the following procedure to create a DHCP scope for the IP telephones.

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP Servers window by double clicking it until the **+** sign changes to a **-** sign.
3. Select **Scope**-->**Create**.
4. Using information recorded in Table 3: Required Network Information Before Installation - Per DHCP Server:

   Define the **Telephone IP Address Range**.

   Set the **Subnet Mask**.

   To ***exclude*** any IP addresses you do not want assigned to IP telephones within the **Start** and **End** addresses range:

   a. In the **Exclusion Range Start Address** field, enter the ***first IP Address*** in the range that you want to exclude.

   b. In the **Exclusion Range End Address** field, enter the ***last IP Address*** in the range that you want to exclude.

   c. Click the **Add** button.

   d. Repeat steps a. through c. for each IP address range to be excluded.

   Note:

   Avaya recommends that you provision the 9600 Series IP Telephones with sequential IP addresses. Also do not mix 9600 Series IP Telephones and PCs in the same scope.

5. Under **Lease Duration**, select the **Limited To** option and set the ***lease duration*** to the maximum.
6. Enter a ***sensible name*** for the **Name** field, such as “DEFINITY IP Telephones.”
7. Click **OK**.

   A dialog box prompts you: `Activate the new scope now?`

8. Click **No**.

   Note:

   Activate the scope only after setting all options.

Editing Custom Options

Use the following procedure to edit custom options.

1. Highlight the newly created scope.
2. Select **DHCP Options**-->**Defaults** in the menu.
3. Click the **New** button.
4. In the **Add Option Type** dialog box, enter an appropriate custom option name, for example, “9600OPTION.”
5. Change the **Data Type Byte** value to **String**.
6. Enter **242** in the **Identifier** field.
7. Click the **OK** button.

   The **DHCP Options** menu displays.
8. Select the **Option Name** for 242 and set the *value string*.
9. Click the **OK** button.
10. For the **Option Name** field, select **003 Router** from the drop-down list.
11. Click **Edit Array**.
12. Enter the ***Gateway IP Address*** recorded in Table 3: Required Network Information Before Installation - Per DHCP Server for the **New IP Address** field.
13. Select **Add** and then **OK**.

Adding the DHCP Option

Use the following procedure to add the DHCP option.

1. Highlight the scope you just created.
2. Select **Scope** under **DHCP Options**.
3. Select the **242** option that you created from the **Unused Options** list.
4. Click the **Add** button.
5. Select option **003** from the **Unused Options** list.
6. Click the **Add** button.
7. Click the **OK** button.
8. Select the **Global parameter** under **DHCP Options**.
9. Select the **242** option that you created from the **Unused Options** list.
10. Click the **Add** button.
11. Click the **OK** button.

Activating the Leases

Use the following procedure to activate the leases.

- Click **Activate** under the **Scope** menu.

  The light-bulb icon for the scope lights.

Verifying Your Configuration

This section describes how to verify that the **96XXOPTIONs** are correctly configured for the Windows NT® 4.0 DHCP server.

Note:

Although this configuration represents that for 9600 Series IP Telephones, the file remains as 46XXOPTIONS. This allows shared use for both 4600 and 9600 Series IP Telephones.

Verify the Default Option, 242 96XXOPTION

1. Select **Start**-->**Programs**-->**Admin Tools**-->**DHCP Manager**.
2. Expand **Local Machine** in the DHCP servers window by double clicking until the **+** sign changes to a **-** sign.
3. In the DHCP servers frame, click the *scope* for the IP telephone.
4. Select **Defaults** from the **DHCP_Options** menu.
5. In the **Option Name** pull-down list, select **242 96XXOPTION**.
6. Verify that the **Value String** box contains the correct string from DHCP Server Administration.

   If not, update the string and click the **OK** button twice.

Verify the Scope Option, 242 96XXOPTION

1. Select **Scope** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct string from DHCP Generic Setup on page 36.

   If not, update the string and click the **OK** button.

Verify the Global Option, 242 96XXOPTION

1. Select **Global** under **DHCP OPTIONS**.
2. In the **Active Options:** scroll list, click **242 96XXOPTION**.
3. Click the **Value** button.
4. Verify that the **Value String** box contains the correct value from DHCP Generic Setup on page 36.

   If not, update the string and click the **OK** button.

Windows 2000 DHCP Server

Verifying the Installation of the DHCP Server

Use the following procedure to verify whether the DHCP server is installed.

1. Select **Start**-->**Program**-->**Administrative Tools**-->**Computer Management**.
2. Under **Services and Applications** in the Computer Management tree, find **DHCP**.
3. If DHCP is not installed, install the DHCP server. Otherwise, proceed directly to Creating and Configuring a DHCP Scope for instructions on server configuration.

Creating and Configuring a DHCP Scope

Use the following procedure to create and configure a DHCP scope.

1. Select **Start**-->**Programs**-->**Administrative Tools**-->**DHCP**.
2. In the console tree, click the *DHCP server* to which you want to add the DHCP scope for the IP telephones. This is usually the name of your DHCP server machine.
3. Select **Action**-->**New Scope** from the menu.

   Windows displays the **New Scope Wizard** to guide you through rest of the setup.
4. Click the **Next** button.

   The **Scope Name** dialog box displays.
5. In the **Name** field, enter a name for the scope such as “DEFINITY IP Telephones,” then enter a brief comment in the **Description** field.
6. When you finish Steps 1 - 5, click the **Next** button.

   The **IP Address Range** dialog box displays.
7. Define the range of IP addresses used by the IP telephones listed in Table 3: Required Network Information Before Installation - Per DHCP Server. The **Start IP Address** is the first IP address available to the IP telephones. The **End IP Address** is the last IP address available to the IP telephones.

   Note:

   Avaya recommends not mixing 9600 Series IP Telephones and PCs in the same scope.

8. Define the **subnet mask** in one of two ways:
   - The number of bits of an IP address to use for the network/subnet IDs.
   - The subnet mask IP address.

   Enter only one of these values. When you finish, click the **Next** button.

   The **Add Exclusions** dialog box displays.
9. Exclude any IP addresses in the range specified in the previous step that you do not want assigned to an IP telephone.
   a. In the **Start Address** field under **Exclusion Range**, enter the ***first IP Address*** in the range you want to exclude.
   b. In the **End Address** field under **Exclusion Range**, enter the ***last IP Address*** in the range you want to exclude.
   c. Click the **Add** button.
   d. Repeat steps a. through c. for each IP address range that you want to exclude.

   Note:

   You can add additional exclusion ranges later by right clicking the **Address Pool** under the newly created scope and selecting the **New Exclusion Range** option.

   Click the **Next** button after you enter all the exclusions.

   The **Lease Duration** dialog box displays.
10. For all telephones that obtain their IP addresses from the server, enter **30 days** in the **Lease Duration** field. This is the duration after which the IP address for the device expires and which the device needs to renew.
11. Click the **Next** button.

    The **Configure DHCP Options** dialog box displays.
12. Click the **No, I will activate this scope later** button.

    The **Router** (Default Gateway) dialog box displays.
13. For each router or default gateway, enter the ***IP Address*** and click the **Add** button.

    When you are done, click the **Next** button.

    The **Completing the New Scope Wizard** dialog box displays.
14. Click the **Finish** button.

    The new scope appears under your server in the DHCP tree. The scope is not yet active and does not assign IP addresses.
15. Highlight the newly created scope and select **Action**-->**Properties** from the menu.

16. Under **Lease duration for DHCP clients**, select **Unlimited** and then click the **OK** button.

    CAUTION:

    IP address leases are kept active for varying periods of time. To avoid having calls terminated suddenly, make the lease duration unlimited.

Adding DHCP Options

Use the following procedure to add DHCP options to the scope you created in the previous procedure.

1. On the DHCP window, right-click the **Scope Options** folder under the scope you created in the last procedure.

   A drop-down menu displays.

2. In the left pane of the DHCP window, right click the **DHCP Server name**, then click **Set Predefined Options...**.
3. Under **Predefined Options and Values**, click **Add**.
4. In the **Option Type Name** field, enter ***any appropriate name***, for example, “Avaya IP Telephones.”
5. Change the **Data Type** to **String**.
6. In the **Code** field, enter **242**, then click the **OK** button twice.

   The **Predefined Options and Values** dialog box closes, leaving the DHCP dialog box enabled.

7. Expand the newly created scope to reveal its **Scope Options**.
8. Click **Scope Options** and select **Action**-->**Configure Options** from the menu.
9. In the **General** tab page, under the **Available Options**, check the **Option 242** checkbox.
10. In the **Data Entry** box, enter the ***DHCP IP telephone option string*** as described in DHCP Generic Setup on page 36.

    Note:

    You can enter the text string directly on the right side of the **Data Entry** box under the ASCII label.

11. From the list in **Available Options**, check option **003 Router**.
12. Enter the ***gateway (router) IP Address*** from the IP address field of Table 3: Required Network Information Before Installation - Per DHCP Server.
13. Click the **Add** button.
14. Click the **OK** button.

Activating the New Scope

Use the following procedure to activate the new scope.

1. In the DHCP console tree, click the **IP Telephone Scope** you just created.
2. From the **Action** menu, select **Activate**.

   The small red down arrow over the scope icon disappears, indicating that the scope was activated.

HTTP Generic Setup

You can store the same application software, script file, and settings file on an HTTP server as you can on a TFTP server. TFTP is not supported for 9600 Series IP Telephones. With proper administration, the telephone seeks out and uses that material. Some functionality might be lost by a reset if the HTTP server is unavailable. For more information, see DHCP and File Servers on page 35.

CAUTION:

The files defined by HTTP server configuration must be accessible from all IP telephones invoking those files. Ensure that the file names match the names in the upgrade script, including case, since UNIX systems are case-sensitive.

Note:

Use any HTTP application you want. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

Important:

You must use the Avaya Web configuration server to obtain HTTPS so information is authenticated.

The Avaya Web configuration server does not support backup/restore. If you intend to use HTTP for backup/restore purposes, you must use an HTTP server that is independent of the Avaya Web configuration server.

To set up an HTTP server:

- Install the HTTP server application.
- Administer the system parameters HTTPSRVR and CODESRVR to the address(es) of the HTTP server. Include these parameters in DHCP Option 242, or the appropriate SSON Option.

- Download the upgrade script file and application file(s) from the Avaya Web site http://www.avaya.com/support to the HTTP server. For more information, see Contents of the Settings File on page 56.

  Note:

  Many LINUX servers distinguish between upper and lower case names. Ensure that you specify the settings file name accurately, as well as the names and values of the data within the file.

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you also need to:

- Install the TLS server application.
- Administer the system parameter TLSSRVR to the address(es) of the Avaya HTTP server.

HTTP Configuration for Backup/Restore

For IIS Web Servers

For IIS 4.0 (WinNT4.0), IIS 5.0 (Win2000), IIS 5.1 (WinXP), IIS 6.0 (Win2003):

1. Create a “backup” folder under the root directory of your Web server. All backup files will be stored in that directory.

   For example, if your backup folder is **C:/Inetpub/wwwroot/backup** the 46xxsettings.txt file should have a line similar to:

   ```
   [SET BRURI http://www.website.com/backup/]
   ```

   If your backup folder is the root directory, the 46xxsettings.txt file should have a line similar to:

   ```
   [SET BRURI http://www.website.com/]
   ```

2. Use **Internet Information Services Manager** or **Internet Information Services** depending on your OS. Go to **Start** --> **Settings** --> **Control Panel** --> **Administrative Tools**.
3. Right click on the folder created for backup, or right click on **Default Web Site** if there is no specific backup directory.
4. Select **Properties**.
5. In the Directory tab, make sure the **Write** box is checked.

Additional step for IIS 6.0 (Win2003):

1. Use **Internet Information Services**. Go to **Start** --> **Settings** --> **Control Panel** --> **Administrative Tools**.
2. Below Default Web Site select **Web Services Extension**.
3. Make sure the WebDAV option is set to **Allowed**.

For Apache Web servers:

1. Create a “backup” folder under the root directory of your Web server, and **make the folder writable by everyone**. All backup files will be stored in that directory.

   If your backup folder is for instance **C:/Program Files/Apache Group/Apache2/htdocs/backup**, the 46xxsettings.txt file should have a line similar to:

   ```
   [SET BRURI http://www.website.com/backup/]
   ```

   If your backup folder is the root directory, the 46xxsettings.txt file should have a line similar to:

   ```
   [SET BRURI http://www.website.com/]
   ```

2. Edit your Web server configuration file **httpd.conf**.
3. Uncomment the two LoadModule lines associated with DAV:

   ```
   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so
   ```

   Note:

   If these modules are not available on your system, typically the case on some Unix/Linux Apache servers, you have to recompile these two modules (mod_dav & mod_dav_fs) into the server. Other ways to load these modules might be available. Check your Apache documentation at http://httpd.apache.org/docs/ for more details.

4. Add the following lines in the **httpd.conf** file:

   ```
   #
   # WebDAV configuration
   #
   DavLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
     <Location />
     Dav On
     </Location>
   ```

   For Unix/Linux Web servers the fourth line might look more like:

   ```
   DavLockDB/usr/local/apache2/var/DAVLock
   ```

5. Create the var directory and **make it writable by everyone**. Right click **Properties**-->**Security**-->**Add**-->**Everyone**-->**Full Control**.

Web Configuration Tool

Recent call server versions provide all the Web configuration support the 9600 Series IP Telephones require. Also, the media server has an easy to use, PC-based interface for creating script files. Given these resources, you do not need to manually create the text files discussed in 9600 Series IP Telephone Scripts and Application Files. For more information about the media server, see *Installation and Upgrades for Avaya G700 Media Gateway and Avaya S8300 Media Server*, available on the Avaya support Web site.

Table 7: 9600 Series IP Telephone Customizable System Parameters lists the parameters you can administer when manually creating the configuration file. Manual administration is discussed in 9600 Series IP Telephone Scripts and Application Files. When using the media server, you do not need to know the specific parameter names, since the media server handles that. For more information, Table 6 lists the parameter names from 9600 Series IP Telephone Customizable System Parameters and the corresponding field name from the media server HTTP server application. Any limits, restrictions, etc. about the parameters are built into the media server.

Note:

The Web Configuration application covers other IP telephones. This document covers only data applicable to 9600 Series IP Telephones.

Table 6: Media Server Field Names & Corresponding Script File Parameter Names

Media Server Field Name	Script File Parameter Name
Handset Audio Gain Control Status	AGCHAND
Headset Audio Gain Control Status	AGCHEAD
Speaker Audio Gain Control Status	AGCSPKR
Application Status	APPSTAT
Script File Server Authentication **Note:** Applicable only when configuration file downloaded using HTTPS. Not applicable if file downloaded using HTTP.	AUTH
Idle Time Before Backlight Turnoff	BAKLIGHTOFF
Backup and Restore URI	BRURI
CNA Server Addresses	CNASRVR
CNA Port Number	CNAPORT

1 of 3

Table 6: Media Server Field Names & Corresponding Script File Parameter Names (continued)

Media Server Field Name	Script File Parameter Name
802.1X Supplicant Mode	DOT1X
DHCP Lease Violation Flag	DHCPSTD
Domain Name	DOMAIN
Domain Name Server	DNSSRVR
HTTP Server IP Address	HTTPSRVR
HTTP Directory	HTTPDIR
Send Destination Unreachable Messages	ICMPDU
Process Received Redirect Messages	ICMPRED
Layer 2 Frame Tagging	L2Q
802.1A VLAN Identifier	L2QVLAN
System-Wide Language	LANGSYS
English Language Selection Status	LANG0STAT
Language File Name	LANGxFILE (with x being 1-4)
Event Log Security Level	LOGLOCAL
Syslog Server Address	LOGSRVR
Management Complex IP Addresses	MCIPADD
Voice Mail Telephone Number	MSGNUM
User Options Access	OPSTAT
Telephone Country Code	PHNCC
Telephone Dial Plan Length	PHNDPLENGTH
International Access Code	PHNIC
Long Distance Access Code	PHNLD
National Telephone # Length	PHNLDLENGTH
Outside Line Access Code	PHNOL
Ethernet Line Interface Status	PHY1STAT

2 of 3

Table 6: Media Server Field Names & Corresponding Script File Parameter Names (continued)

Media Server Field Name	Script File Parameter Name
Secondary Ethernet Interface Layer 2 Priority Value	PHY2PRIO
Secondary Ethernet Line Interface Status	PHY2STAT
Secondary Ethernet Interface VLAN Identifier	PHY2VLAN
Local (dial pad) Procedure Password	PROCPSWD
Local Dialpad Procedures Allowed	PROCSTAT
Reregistration Timer	REREGISTER
RTCP Monitor IP Address	RTCPMON
Screen Saver	SCREENSAVERON
Source IP Addresses for SNMP Queries	SNMPADD
SNMP Community String	SNMPSTRING
Subscription List	SUBSCRIBELIST
Trusted Domains/Paths	TPSLIST
Unnamed Registration Status	UNNAMEDSTAT
Secondary Ethernet Interface Layer 2 Frame Tagging	VLANSEP
Wait Time for DHCP Offer	VLANTEST
9600 Home Page	WMLHOME
9600 HTTP Proxy Server	WMLPROXY
9600 HTTP Proxy Server Port	WMLPORT
9600 HTTP Proxy Server Exception Domains	WMLEXCEPT
Idle Time Before Web Page Display	WMLIDLETIME
Idle Time Web Page Display	WMLIDLEURI

3 of 3

Chapter 6: Telephone Software and Application Files

General Download Process

The 9600 Series IP Telephones download script files, application files, and settings files from either an HTTP or HTTPS server. The HTTPS server applies only if the server supports Transport Layer Security (TLS) encryption.

Note:

The script files, application files, and settings files discussed in this chapter are identical for HTTP and HTTPS servers. The generic term “file server” refers to both “HTTP server” and “HTTPS server.”

The file downloading process is the same for both servers, except when you use an HTTPS server, a TLS server is contacted first. The telephone queries the file server, which transmits a script file to the telephone. The script file tells the telephone which application file the telephone must use. The application file is the software that has the telephony functionality, and is easily updated for future enhancements. In a newly installed telephone, the application file might be missing. In a previously installed telephone, the application file might not be the proper one. In both cases, the telephone requests a download of the proper application file from the file server. The file server downloads the file and conducts some checks to ensure that the file was downloaded properly. If the telephone determines it already has the proper file, the telephone proceeds to the next step without downloading the application file again.

After checking and loading the application file, the 9600 Series IP Telephone, if appropriate, uses the script file to look for a settings file. The settings file contains options you have administered for any or all of the 9600 Series IP Telephones in your network. For more information about the settings file, see Contents of the Settings File on page 56.

Software

When shipped from the factory, the 9600 Series IP Telephones might not contain sufficient software for registration and operation. When the telephone is first plugged in, a software download from an HTTP or HTTPS server starts to give the phone its proper functionality.

For software upgrade downloads, the call server provides the capability for a remote restart of the 9600 Series IP Telephone. As a result of restarting, the telephone automatically starts reboot procedures. If new software is available on the server, the telephone downloads it as part of the reboot process. The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* covers upgrades to a previously installed telephone and related information.

9600 Series IP Telephone Scripts and Application Files

Choosing the Right Application File and Upgrade Script File

The software releases containing the files needed to operate the 9600 Series IP Telephones are bundled together. You download this self-extracting executable file to your file server from the Avaya support Web site at: http://www.avaya.com/support. The file is available in both zipped and unzipped format.

The bundle contains:

- An upgrade script file and a settings file, which allow you to upgrade to new software releases and new functionality without having to replace IP telephones.
- Application files for all current 9600 Series IP Telephones.
- Other useful information such as a ReadMe file and a settings file template to customize parameters and settings, and the latest binary code.

Upgrade Script File

An upgrade script file tells the IP telephone whether the telephone needs to upgrade software. The Avaya IP Telephones attempt to read this file whenever they reset. The upgrade script file also points to the settings file.

You download a default upgrade script file, sometimes called the “script file,” from http://www.avaya.com/support. This file allows the telephone to use default settings for customer-definable options. This file must reside in the same directory as the upgrade script file, and must be called ***46xxsettings.txt***.

Note:

Avaya recommends that the settings file have the extension ***.txt**. The Avaya IP Telephones can operate without this file. You can also change these settings with DHCP or, in some cases, from the dialpad of the telephone.

Settings File

The settings file contains the option settings you need to customize the Avaya IP Telephones for your enterprise.

Note:

You can use one settings file for all your Avaya IP Telephones. The settings file includes the 9600 Series IP Telephones covered in this document and 4600 Series IP Telephones, as covered in the *4600 Series IP Telephone LAN Administrator Guide* (Document 555-233-507).

The settings file can include any of five types of statements, one per line:

- Comments, which are statements with a "#" character in the first column.
- Tags, which are comments that have exactly one space character after the initial #, followed by a text string with no spaces.
- `Goto` commands, of the form **GOTO *tag.*** `Goto` commands cause the telephone to continue interpreting the configuration file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the configuration file is ignored.
- Conditionals, of the form **IF *$name* SEQ *string* GOTO *tag***. Conditionals cause the `Goto` command to be processed if the value of ***name*** is a case-insensitive equivalent to ***string***. If no such ***name*** exists, the entire conditional is ignored. The only system values that can be used in a conditional statement are: BOOTNAME, GROUP, and SIG.
- `SET` commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric, a dotted decimal IP address, and so on.

Note:

Enclose all data in quotation marks for proper interpretation.

The upgrade script file Avaya provides includes a line that tell the telephone to **GET *46xxsettings.txt***. This lines causes the telephone to use HTTP to attempt to download the file specified in the `GET` command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the telephone continues processing the upgrade script file.

If the configuration file is successfully obtained but does not include any setting changes the telephone stops using HTTP. This happens when you initially download the script file template from the Avaya support Web site, before you make any changes. When the configuration file contains no setting changes, the telephone does not go back to the upgrade script file.

Avaya recommends that you do **not** alter the upgrade script file. If Avaya changes the upgrade script file in the future, any changes you have made will be lost. Avaya recommends that you use the ***46xxsettings*** file to customize your settings instead. However, you can change the settings file name, if desired, as long as you also edit the corresponding `GET` command in the upgrade script file.

For more information on customizing your settings file, see Contents of the Settings File.

Contents of the Settings File

After checking the application software, the 9600 Series IP Telephone looks for a 46xxsettings file. This optional file is where you identify non-default option settings, application-specific parameters, and so on. You can download a template for this file from the Avaya support Web site. An example of what the file might look like follows.

Note:

The following is intended only as a simple example. Your settings will vary from the settings shown. This sample assumes specification of a DNS Server, turning off enhanced local dialing, and a Web Browser.

DNSSRVR=”dnsexample.yourco.com”

ENDIALSTAT=0

WMLHOME=”http://yourco.com/home.wml”
WMLPROXY=”11.11.11.11”

See Chapter 7: Administering Telephone Options for details about specific values. You need only specify settings that vary from defaults, although specifying defaults is harmless.

VLAN separation controls whether or not traffic received on the secondary Ethernet interface are forwarded on the voice VLAN and whether network traffic received on the data VLAN are forwarded to the telephone. Add commands to the 46xxsettings.txt file to enable VLAN separation. The following example assumes the voice VLAN ID is “xxx”, the data VLAN ID is “yyy” and the data traffic priority is “z”:

SET VLANSEP 1
SET L2Q 1 (or 0 for auto)
SET L2QVLAN xxx
SET PHY2VLAN yyy
SET PHY2PRIO z

Note:

Also configure the network switch so that 802.1Q tags are not removed from frames forwarded to the telephone.

The GROUP System Value

You might have different communities of users, all of which have the same telephone model, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to Logoff, which might be an essential capability for “hot-desking” associates. We provide examples of the group settings for each of these situations later in this section.

Use the GROUP system value for this purpose:

1. identify which telephones are associated with which group, and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group is assigned as Group 0.
2. At each non-default telephone, instruct the installer or user to invoke the GROUP Local (dialpad) Administrative procedure as specified in the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* and specify which GROUP number to use. The GROUP System value can only be set on a phone-by-phone basis.
3. Once the GROUP assignments are in place, edit the configuration file to allow each telephone of the appropriate group to download its proper settings.

Here is an example of the configuration file for the Call Center agent:

```
IF $GROUP SEQ 1 goto CALLCENTER
IF $GROUP SEQ 2 goto HOTDESK
{specify settings unique to Group 0}
goto END

# CALLCENTER
{specify settings unique to Group 1}
goto END

# HOTDESK
{specify settings unique to Group 2}

# END
{specify settings common to all Groups}
```

Chapter 7: Administering Telephone Options

Administering Options for the 9600 Series IP Telephones

This chapter explains how to change parameters by means of the DHCP or HTTP servers. In all cases, you are setting a system parameter in the telephone to a desired value. Table 7 lists:

- the parameter names,
- their default values,
- the valid ranges for those values, and
- a description of each one.

For DHCP, the DHCP Option sets these parameters to the desired values as discussed in DHCP and File Servers on page 35. For HTTP, the parameters in Table 7 are set to desired values in the script file. For more information, see Contents of the Settings File on page 56. When using a media server, see Table 6: Media Server Field Names & Corresponding Script File Parameter Names on page 50 for information on parameters set by the media server application.

Avaya recommends that you administer options on the 9600 Series IP Telephones using script files. Some DHCP applications have limits on the amount of user-specified information. The administration required can exceed those limits for the more full-featured telephone models.

You might choose to completely disable the capability to enter or change option settings from the dialpad. You can set the system value, PROCPSWD, as part of standard DHCP/HTTP administration. If PROCPSWD is non-null and consists of 1 to 7 digits, the user cannot invoke any “dialpad options” without first pressing **Mute** or **Hold** and entering the PROCPSWD value. For more information on dialpad options, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

CAUTION:

PROCPSWD is likely stored on the server “in the clear” and is sent to the telephone in the clear. Therefore, do not consider PROCPSWD as a high-security technique to inhibit a sophisticated user from obtaining access to local procedures.

Administering this password can limit access to all local procedures, including V I E W. VIEW is a read-only option that allows review of the current telephone settings.

Table 7: 9600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Description and Value Range
AGCHAND	1	Automatic Gain Control status for handset (0=disabled, 1=enabled).
AGCHEAD	1	Automatic Gain Control status for headset (0=disabled, 1=enabled).
AGCSPKR	1	Automatic Gain Control status for Speaker (0=disabled, 1=enabled).
APPNAME	" " (Null)	Primary application image file name, as provided in the 9600upgrade.txt file.
APPSTAT	1	Controls whether specific applications are enabled, restricted, or disabled. Values are: 1=all applications enabled, 2=Speed Dial (Contacts) changes and Call Log disabled and Redial last number only, 3=Speed Dial (Contacts) changes disabled, 0=Speed Dial (Contacts) changes, Call Log, and Redial disabled.
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
BAKLIGHTOFF	120	Number of minutes without display activity to wait before turning off the backlight. Values: 0-999, no spaces and no null value. A value of 0 means the backlight never turns off.
BRURI	" " (Null)	URL used for backup and retrieval of user data. Specify HTTP server and directory path to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and spaces are allowed.
CNAPORT	50002	Avaya Converged Network Analyzer (CNA) server registration transport-layer port number (0-65535).
CNASRVR	“ ” (Null)	Text string containing the IP addresses of one or more Avaya Converged Network Analyzer (CNA) servers to be used for registration. Format is dotted decimal or DNS format, separated by commas, with no spaces (0-255 ASCII characters, including commas).
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP address if there is no response to lease renewal. If set to “1” (No) the telephone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to “0” (Yes) the telephone continues using the IP address until it detects reset or a conflict (see DHCP Generic Setup).
DNSSRVR	0.0.0.0	Text string containing the IP address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces (0-255 ASCII characters, including commas).
DOMAIN	" " (Null)	Text string containing the domain name to be used when DNS names in system values are resolved into IP addresses. Valid values are 0-255 ASCII characters. If Null, no spaces allowed.

1 of 6

Table 7: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
DOT1X	0	802.1X Supplicant operation mode. Valid values are: 0=With PAE pass-through, 1=with PAE pass-through and proxy Logoff, 2=without PAE pass-through or proxy Logoff.
ENHDIALSTAT	1	Enhanced Dialing Status. If set to “1” the Enhanced Local Dialing feature is turned on for all associated applications. If set to “0” the feature is turned off.
HTTPDIR	" " (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP and HTTPS get operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required.
HTTPSRVR	" " (Null)	Text list of HTTP server addresses in dotted decimal or DNS format, separated by commas (0-255 ASCII characters, including commas).
ICMPDU	0	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages, 2=Send Protocol and Port Unreachable messages.
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: 0=No, 1=Yes.
L2Q	0	Controls whether Layer 2 frames have IEEE 802.1Q tags (0=auto, 1=enabled, 2=disabled).
L2QVLAN	0	802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. VLAN identifier used by IP telephones. Set this parameter only when IP telephones are to use a VLAN that is separate from the default data VLAN. If the VLAN identifier is to be configured via H.323 signaling based on Avaya Communication Manager administration forms, it should not be set here.
LANG0STAT	1	Controls whether the built-in English language text strings can be selected by the user. Valid values are: 0 = User cannot select English language text strings 1 = User can select English language text strings/
LANGxFILE	" " (Null)	Name of the language file in use: LANG1FILE = LANG2FILE = LANG3FILE = LANG4FILE =
LANGSYS	" " (Null)	0 to 32 ASCII characters. The file name of the system default language file, if any.

2 of 6

Table 7: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
LOGLOCAL	0	Event Log Severity Level (one 0-8 ASCII numeric digit). Controls the level of events logged in the endptRecentLog and endptResetLog objects in the SNMP MIB. Events with the selected level and with a higher severity level will be logged. Valid values are: 0=Disabled, 1=emergencies, 2=alerts, 3=critical, 4=errors, 5=warnings, 6=notices, 7=information, 8=debug.
LOGSRVR	" " (Null)	Voice Monitoring Manager (VMM) Server Address. Zero or one IP address in dotted-decimal format or DNS Name format (0-15 ASCII characters).
MCIPADD	0.0.0.0	Call Server Address. Zero or more Avaya Communication Manager server IP addresses. Format is dotted-decimal or DNS name format, separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
MSGNUM	" " (Null)	Voice mail telephone number. Specifies the number to be dialed automatically when the telephone user presses the **Message** button. Value: 0-30 ASCII dialable characters (0-9, * and #) and no spaces. Null is a valid value.
OPSTAT	111	Options status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as noted in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows full display and access to all options and related applications.
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from “1” to “999.”
PHNDPLENGTH	5	Internal extension telephone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “10.”

3 of 6

Table 7: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PHNIC	011	Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 digit or " " (Null).
PHNLDLENGTH	10	Length of national telephone number. The number of digits in the longest possible national telephone number by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from “3” to “10.” Range: 1 or 2 ASCII numeric characters, from “5” to “15.”
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-2 dialable characters, including " " (Null).
PHY1STAT	1	Ethernet line interface setting (1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex, and 6=1000Mbps full-duplex if supported by the hardware).
PHY2PRIO	0	Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Values are from 0-7 and correspond to the drop-down menu selection.
PHY2STAT	1	Secondary Ethernet interface setting (0=Secondary Ethernet interface off/disabled, 1=auto-negotiate, 2=10Mbps half-duplex, 3=10Mbps full-duplex, 4=100Mbps half-duplex, 5=100Mbps full-duplex), and 6=1000Mbps full-duplex if supported by the hardware).
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is "1" (enabled). Value is 1-4 ASCII numeric digits from “0” to “4094.” Null is not a valid value, nor can the value contain spaces.
PROCPSWD	" " (Null)	Text string containing the local (dialpad) procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after Mute is pressed and before entry of a procedure command (for example, VIEW). Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.

4 of 6

Table 7: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
PROCSTAT	0	Local (dialpad) Administrative procedures status (0=Local procedures enabled, 1=all Administrative Options are disabled).
REREGISTER	20	Registration timer in minutes. Controls an H.323 protocol timer that should only be changed under very special circumstances by someone who fully understands the system operation impact. Value is 1-120.
RTCPMON	" " (Null)	Text string containing the 4-octet IP address of the RTCP monitor currently in use, in dotted decimal or DNS Name format (0-15 ASCII characters, no spaces).
SCREENSAVERON	60	Number of idle time minutes after which the screen saver is turned on. Valid values are 1-3 ASCII numeric digits, 0-999.
SNMPADD	" " (Null)	Text string containing zero or more allowable source IP addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas.
SNMPSTRING	" " (Null)	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces).
STATIC	0	Static programming override flag. If set to “0” static programming never overrides call server (DHCP) or call server administered data. If set to “1” static programming overrides only file server administered data. If set to “2” static programming overrides only call server administered data. If set to “3” static programming overrides both file server- and call server-administered data. Allows a call server IP address that has been manually programmed into a telephone to override any value received via DHCP or via this configuration file. A manually programmed IP address will only be used if it is not 0.0.0.0, so this parameter may be used to allow only specific telephones to use a different value than otherwise provided by this configuration file. If STATIC is to be used to select a manual override of file server IP address(es), STATIC must be set via DHCP, not via this configuration file.
SUBSCRIBELIST	" " (Null)	One or more Push application server subscription URLs, separated by commas without any intervening spaces (0-255 ASCII characters, including commas).
TPSLIST	" " (Null)	One or more trusted domain/path strings, separated by commas without any intervening spaces (0-255 ASCII characters, including commas). A URL pushed to a telephone must contain one of these strings if it is to be used to obtain content to be rendered by the telephone.

5 of 6

Table 7: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Description and Value Range
UNNAMEDSTAT	1	Unnamed Registration Status. Specifies whether unnamed registration is initiated if the user fails to enter a value at the `Extension:` prompt or Login screen. Unnamed registration provides the telephone with a TTI-level service, enabling a user, for example, to dial emergency services like 911. Value 1=Yes, 0=No.
VLANSEP	1	VLAN separation. Controls whether frames to/from the secondary Ethernet interface receive IEEE 802.1Q tagging treatment. The tagging treatment enables frames to be forwarded based on their tags in a manner separate from telephone frames. If tags are not changed, no tag-based forwarding is employed. Values are: 1=On/Enabled, 2= Off/Disabled. This parameter is used with several related parameters. For more information, see VLAN Separation on page 67.
VLANTEST	60	Number of seconds to wait for a DHCPOFFER when using a non-zero VLAN ID (1-3 ASCII digits, from “0” to “999”).
WMLEXCEPT	" " (Null)	One or more HTTP proxy server exception domains that do not require the use of the proxy server (0-127 ASCII characters, including commas, without any intervening spaces). Set this parameter only if a proxy server is used and if there are exception domains.
WMLHOME	" " (Null)	URL that specifies the home page for Web browsers that use WML. Zero or one URL (0-255 ASCII characters, including spaces, if any). If Null, the Web application will not be displayed.
WMLIDLETIME	10	Idle time before displaying Web page. Number of minutes without activity to wait before displaying the idle Web page. Value: 1-999 with no spaces. Null is not a valid value.
WMLIDLEURI	" " (Null)	Idle time Web page URI. URI that specifies the Web page the browser displays after an idle interval. Value: Zero or one URI (0-255 ASCII characters, no spaces). Null is valid but if Null, no page displays.
WMLPORT	8000	TCP port number for the HTTP proxy server, if applicable (1-5 ASCII numeric characters from “0” to “65535.” Null is not a valid value.
WMLPROXY	" " (Null)	One HTTP proxy server IP address in dotted decimal or DNS Name format (0-255 ASCII characters). Set this parameter only if Web pages requiring a proxy server will be supported.

6 of 6

Note:

Table 7 applies to all 9600 Series IP Telephones. Certain 9600 IP Telephones might have additional, optional information that you can administer. For more information, see Chapter 8: Administering Applications and Options.

VLAN Considerations

If your LAN environment does not include Virtual LANs (VLANs), ignore this section. Otherwise, this section contains information on how to administer 9600 Series IP Telephones to minimize registration time and maximize performance in a VLAN environment.

VLAN Default Value and Priority Tagging

The system value **L2QVLAN** is initially set to “0” and identifies the 802.1Q VLAN Identifier. This default value indicates “priority tagging” as defined in IEEE 802.IQ Section 9.3.2.3. Priority tagging specifies that your network closet Ethernet switch automatically insert the switch port default VLAN without changing the user priority of the frame (cf. IEEE 802.1D and 802.1Q).

If you do not want the default VLAN to be used for voice traffic:

- Ensure that the switch configuration lets frames tagged by the 9600 Series IP Telephone through without overwriting or removing them.
- Set the system value **L2QVLAN** to the ***VLAN ID*** appropriate for your voice LAN.

Another system value you can administer is **VLANTEST**. VLANTEST defines the number of seconds the 9600 IP Series Telephone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is “60” seconds. Using VLANTEST ensures that the telephone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid. The default value is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, etc. to be returned to service. If the telephone restarts for any reason and the VLANTEST time limit expires, the telephone assumes the administered VLAN ID is invalid. The telephone then initiates registration with the default VLAN ID.

Setting **VLANTEST** to “**0**” has the special meaning of telling the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the telephone does not return to the default VLAN.

Note:

If the telephone returns to the default VLAN but must be put back on the L2QVLAN VLAN ID, you must Reset the telephone. See the Reset procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.

VLAN Separation

VLAN separation controls whether or not traffic received on the secondary Ethernet interface can be forwarded on the voice VLAN. VLAN separation also controls whether network traffic received on the data VLAN can be forwarded to the telephone. The following system parameters control VLAN separation:

- **VLANSEP** - enables (1) or disables (0) VLAN separation. The default is 1 (on), which allows full separation. When set to 0 (off), VLAN IDs are not used as a criteria for forwarding frames.
- **L2Q** - 802.1Q tagging must be set to 1 (on) or 0 (auto).
- **L2QVLAN** - must be set to the non-zero VLAN ID of the voice VLAN.
- **PHY2VLAN** - must be set to the non-zero VLAN ID of the data VLAN, which cannot be the same as the voice VLAN ID.
- **PHY2PRIO** - the layer 2 priority value to be used for tagged frames received on the secondary Ethernet interface.

Table 8 provides several VLAN separation guidelines.

Table 8: VLAN Separation Rules

If		Then
VLANSEP is “0” or "2" (Off/Disabled),	**OR** the telephone is not tagging frames, **OR** the telephone is tagging frames with a VLAN ID equal to PHY2VLAN.	Frames received on the secondary Ethernet interface will not be changed before forwarding. For example, tagging is not added or removed and the VLAN ID and tagged frames priority are not changed. The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.
VLANSEP is “1” (On/Enabled)		All tagged frames received on the secondary Ethernet interface are changed before forwarding to make the VLAN ID equal to the PHY2VLAN value and the priority value equal to the PHY2PRIO value. Untagged frames received on the secondary Ethernet interface are not changed before forwarding.

1 of 2

Table 8: VLAN Separation Rules (continued)

If		Then
VLANSEP is “1” (On/Enabled)	**AND** the telephone is not tagging frames, **OR** if the telephone is tagging frames with a VLAN ID equal to PHY2VLAN, **OR** if the PHY2VLAN value is zero.	The Ethernet switch forwarding logic determines that frames received on the Ethernet line interface are forwarded to the secondary Ethernet interface or to the telephone without regard to specific VLAN IDs or the existence of tags.
VLANSEP is “1” (On/Enabled)	**AND** the telephone is tagging frames with a VLAN ID not equal to PHY2VLAN, **AND** the PHY2VLAN value is not zero.	Tagged frames received on the Ethernet line interface will only be forwarded to the secondary Ethernet interface if the VLAN ID equals PHY2VLAN. Tagged frames received on the Ethernet line interface will only be forwarded to the telephone if the VLAN ID equals the VLAN ID used by the telephone. Untagged frames will continue to be forwarded or not forwarded as determined by the Ethernet switch forwarding logic.

DNS Addressing

The 9600 IP Telephones support DNS addresses and dotted decimal addresses. The telephone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. See DHCP Generic Setup on page 36 for information. At least one address in Option 6 must be a valid, non-zero, dotted decimal address, otherwise, DNS fails. The text string for the **DOMAIN** system parameter (Option 15, Table 7) is appended to the address(es) in Option 6 before the telephone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and/or Domain name in the HTTP script file. But first **SET** the **DNSSRVR** and **DOMAIN** values so you can use those names later in the script.

Note:

Administer Options 6 and 15 appropriately with DNS servers and Domain names respectively.

IEEE 802.1X

Certain 9600 Series IP Telephones support the IEEE 802.1X standard for pass-through and Supplicant operation. The system parameter DOT1X determines how the telephones handle 802.1X multicast packets and proxy logoff, as follows:

- When DOT1X = 0, the telephone forwards 802.1X multicast packets from the Authenticator to the PC attached to the telephone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). Proxy Logoff is not supported.
- When DOT1X = 1, the telephone supports the same multicast pass-through as when DOT1X=0. Proxy Logoff is supported.
- When DOT1X = 2, the telephone forwards multicast packets from the Authenticator only to the telephone, ignoring multicast packets from the attached PC (no multicast pass-through). Proxy Logoff is not supported.
- Regardless of the DOT1X setting, the telephone always properly directs unicast packets from the Authenticator to the telephone or its attached PC, as dictated by the MAC address in the packet.

802.1X Pass-Through and Proxy Logoff

9600 Series IP Telephones with a secondary Ethernet interface support pass-through of 802.1X packets to and from an attached PC. This enables an attached PC running 802.1X supplicant software to be authenticated by an Ethernet data switch.

The IP Telephones support two pass-through modes:

- pass-through and
- pass-through with proxy logoff.

The DOT1X parameter setting controls the pass-through mode. In Proxy Logoff mode (DOT1X=1), when the secondary Ethernet interface loses link integrity, the telephone sends an 802.1X EAPOL-Logoff message to the data switch on behalf of the attached PC. The message alerts the switch that the device is no longer present. For example, a message would be sent when the attached PC is physically disconnected from the IP telephone. When DOT1X = 0 or 2, the Proxy Logoff function is not supported.

802.1X Supplicant Operation

9600 IP Telephones that support Supplicant operation also support Extensible Authentication Protocol (EAP), but only with the MD5-Challenge authentication method as specified in IETF RFC 3748 [8.5-33a].

A Supplicant identity (ID) and password of no more than 12 numeric characters are stored in reprogrammable non-volatile memory. The ID and password are not overwritten by telephone software downloads. The default ID is the MAC address of the telephone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to defaults at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When a telephone is installed for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the Supplicant identity and password. The IP telephone does not accept null value passwords. See “Dynamic Addressing Process” in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*. The IP telephone stores 802.1X credentials when successful authentication is achieved. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP telephone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which it is connected. Some switches may authenticate only a single device per switch port. This is known as single-supplicant or port-based operation. These switches typically send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch.
- **Telephone with attached PC (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch. The attached PC in this scenario gains access to the network without being authenticated.
- **Telephone with attached PC (PC Only Authenticates) -** When the IP telephone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The telephone in this scenario gains access to the network without being authenticated.

Some switches support authentication of multiple devices connected through a single switch port. This is known as multi-supplicant or MAC-based operation. These switches typically send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- **Standalone telephone (Telephone Only Authenticates) -** When the IP telephone is configured for Supplicant Mode (DOT1X=2), the telephone can support authentication from the switch.
- **Telephone and PC Dual Authentication -** Both the IP telephone and the connected PC can support 802.1X authentication from the switch. The IP telephone may be configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1). The attached PC must be running 802.1X supplicant software.

Local Administrative Options Using the Telephone Dialpad

The *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide* details how to use local procedures at the telephone for administration. The local procedures you use most often as an administrator are:

- **CLEAR** - Remove all administered values, user-specified data, option settings, etc. and return a telephone to its initial “out of the box” default values.
- **DEBUG** - Enable or disable debug mode for the button module serial port.
- **GROUP** - Set the group identifier on a per-phone basis.
- **RESET** - Reset the telephone to default values including the registration extension and password, any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- **RESTART** - Restart the telephone in response to an error condition, including the option to reset system values.
- **VIEW** - Review the 9600 IP Telephone system parameters to verify current values and file versions.
- **Secondary Ethernet (Hub) Interface Enable/Disable** - Enable or disable the secondary Ethernet hub locally.

Language Selection

9600 Series IP Telephones are factory-set to display information in the English language. As of Release 1.1, all software downloads include language files for 13 additional languages. Administrators can specify from one to four of those languages per telephone to replace English. End users can then select which of those languages they want their telephone to display.

All downloadable language files contain:

- UTF-16 encoded Unicode characters (only),
- a file name ending in .txt,
- the language name as it should be presented to the user for selection,
- a translation of each available language name into all other languages,
- an indication of the preferred character input method as shown in Table 9,
- text string replacements for the built-in English text strings, for example, entry prompts and error messages, and
- an indication of the font corresponding to the language.

Table 9: Language Files Available with Software Downloads

Language	Character Input Method to be specified in each respective language file	Font
Chinese (Simplified)	Simplified Chinese	Chinese
Dutch	Latin-1	Default
English	Latin-1	Default
French (Canadian)	French	Default
French (Parisian)	French	Default
German	German	Default
Hebrew	Hebrew	Default
Italian	Italian	Default
Japanese (Kanji, Hiragana, and Katakana)	Japanese	Japanese
Korean	Korean	Korean

1 of 2

Table 9: Language Files Available with Software Downloads (continued)

Portuguese (Brazilian)	Portuguese	Default
Russian	Russian	Default
Spanish (Castilian)	Spanish	Default
Spanish (Latin American)	Spanish	Default
		2 of 2

There are no dependencies between the languages available from the software download and the actual character input method. If a character input method is not supported, ASCII is used instead. Acceptable input methods are as follows:

- ASCII
- Latin-1
- German
- French
- Italian
- Spanish
- Portuguese
- Russian
- Albanian, Azeri, Turkish
- Croatian, Slovenian
- Czech, Slovak
- Estonian
- Hungarian
- Latvian
- Lithuanian
- Polish
- Romanian

Use the configuration file and these parameters to customize the settings for up to four languages:

- **LANGxFILE** - The name of a selected language file, for example, "French". In addition to providing the language name as this value, replace the "x" in this parameter with a "1", "2", "3", or "4" to indicate which of four languages you are specifying. For example, to indicate German and French are the available languages, the setting is: **LANG1FILE=mlf_german.txt** and **LANG2FILE=mlf_french.txt**.
- **LANG0STAT** - Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is "0" and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is "1" the user can select the built-in English language text strings.
- **LANGSYS** = The file name of the system default language file, if any.

For more information, see 9600 Series IP Telephone Customizable System Parameters. To view multiple language strings, see the MLS local procedure in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide*.

Note:

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

Gigabit Ethernet Adapter

As of Release 1.1, 9600 Series IP Telephones accommodate a Gigabit Ethernet Adapter. When connected to an adapter interface, the Gigabit Ethernet Adapter sets the Ethernet line interface operational mode that is built into the telephone to 1000Mbps full-duplex and deactivates the built-in secondary Ethernet interface. When a Gigabit Ethernet Adapter is present, any considerations or processing that apply to the "Ethernet line interface" apply only to the Ethernet line interface on that adapter. Likewise, any considerations or processing that apply to the "secondary Ethernet interface" apply only to the secondary Ethernet interface on the Gigabit Ethernet Adapter.

With a Gigabit Ethernet Adapter connected, system parameters PHY1STAT (the Ethernet line interface) and PHY2STAT (the secondary Ethernet interface) activate the respective Ethernet interface in the 1000Mbps operational mode when supported by the hardware. When not supported by the hardware, the respective Ethernet interface is set to auto-negotiate the speed and duplex.

Enhanced Local Dialing

The 9600 Series IP Telephones have a variety of telephony-related applications that might obtain a telephone number during operation. For example, the Call Log saves a number of an incoming caller. The telephones can evaluate a raw telephone number. Based on administered parameters, the telephone can automatically prepend the correct digits, saving the user time and effort. This is the Enhanced Dialing feature. The key to the success of this feature is accurate administration of several important values, summarized below.

Note:

In all cases, the values you administer are the values relevant to the location of the Avaya Media Server at which the IP telephones are registered. If a telephone is in Japan, but its media server is in the United States, set the **PHNCC** value to “1" for the United States.

In all cases, the digits the telephones insert and dial are subject to standard Avaya Media Server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.

As indicated in Table 7, you can administer the system parameter **ENHDIALSTAT** to turn off the Enhanced Local Dialing feature.

The system values relevant to the Enhanced Dialing Feature are:

- **PHNCC** - the international country code of the media server.
  For example, “1” for the United States, “44” for the United Kingdom, and so on.
- **PHNDPLENGTH** - the length of the dial plan on the media server.
- **PHNIC** - the digits the media server dials to access public network international trunks.
  For example, “011” for the United States.
- **PHNLD** - the digit dialed to access public network long distance trunks on the media server.
- **PHNLDLENGTH** - the maximum length, in digits, of the national telephone number for the country in which the Avaya Media Server is located.
- **PHNOL** - the character(s) dialed to access public network local trunks on the media server.

Example: A corporate voice network has a 4-digit dialing plan. The corporate WML Web site lists a 4-digit telephone number as a link on the Human Resources page. A 9620 user selects that link. The 9620 deduces the telephone number is part of the corporate network because the length of the telephone number is the same as the corporate dialing plan. The telephone dials the number without further processing.

Example: A user notes a Web site contains an international telephone number that needs to be called and initiates the call. The telephone determines the number to be called is from another country code. The telephone then prepends the rest of the telephone number with PHNOL to get an outside line and PHNIC to get an international trunk. The telephone then dials normally, with the Avaya Media Server routing the call appropriately.

Note:

The Enhanced Local Dialing algorithm requires that telephone numbers be presented in a standard format. The standard format depends on how you administer the parameters indicated in Table 7. The algorithm also assumes that international telephone numbers are identified as such in, for example, WML Web sites. This is indicated by preceding that type of number with a plus (+) sign, and a space or some non-digit character following the country code.

Backup/Restore

The 9600 Series IP Telephones support the HTTP client to back up and restore the user-specific data indicated in Table 11. For backup, the telephone creates a file with all the user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with appropriate success or failure confirmation.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process, otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with ***/:ddd***, where *ddd* is one to five ASCII numeric digits, the file name is inserted between the forward slash and the colon.
- If BRURI ends with **/** (a forward slash), the file name is appended.
- Otherwise, a forward slash is appended to the BRURI value, then the file name is appended to that.

HTTP authentication is supported for both backup and restore operations. The authentication credentials and realm are stored in re-programmable, non-volatile memory, which is not overwritten when new telephone software is downloaded. Both the authentication credentials and realm have a default value of null, set at manufacture or at any other time user-specific data is removed from the telephone.

The new value(s) replace the currently stored values:

- when HTTP authentication for backup or restore succeeds and
- if the userid, password or realm used differs from those currently stored in the telephone.

If HTTP authentication fails, the user is prompted to enter new credentials.

Note:

Users can request a backup or restore using the Advanced Options Backup/ Restore screen, as detailed in the user guide for their specific telephone model. or specific error messages relating to Backup/Restore, see the *Avaya one-X™ Deskphone Edition for 9600 IP Telephones Installation and Maintenance Guide*.

Backup

When the system parameter BRURI is non-null, user changes are automatically backed up to the file **ext_96xxdata.txt** (where **ext** is the value of NVPHONEXT) on the HTTP server to a user-specified directory. Backup formats are as follows:

Table 10: Backup File Formats

Item/Data Value	Format
Generic	*name=value*
Contacts	ABKNAME*mmm*=ENTRY_NAME ABKNUMBER*mmm*=ENTRY_NUMBER_1 (where *mmm* is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)
User-generated Call Appearance labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	PHNLABEL*mm*=CAUSERLABEL
User-generated telephone Feature Button labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	PHNLABEL*mm*=FBUSERLABEL
User-generated SBM24 Call Appearance or Feature Button labels with button identifiers of *mm* (the one- or two-digit button number of the entry with a lead zero for single-digit numbers)	SBMLABEL*mm*=CAUSERLABEL or FBUSERLABEL, as applicable

In addition to the parameters listed in Table 7, a backup saves the options and non-password parameters shown in Table 11.

Table 11: Options and Non-Password Parameters Saved During Backup

Parameter Name	Setting
LOGACTIVE	Call Log Active
LOGBRIDGED	Log Bridged Calls
OPTAGCHAND	Handset Automatic Gain Control
OPTAGCHEAD	Headset Automatic Gain Control
OPTAGCSPKR	Speaker Automatic Gain Control
OPTAUDIOPATH	Audio Path
OPTCLICKS	Button Clicks
OPTERRORTONE	Error Tones
PERSONALRING	Personalized Ring
PHNREDIAL	Redial
PHNSCRONCALL	Go to Phone Screen on Calling
PHNSCRONALERT	Go to Phone Screen on Ringing
PHNTIMERS	Call Timer
PHNVISUALALERT	Visual Alerting

Restore

When automatic or user-requested retrieval of backup data is initiated, system values and internal values are set to values contained in the backup file. This occurs only if the OPSTAT parameter setting allows the user to change those values. Therefore, any restrictions set using OPSTAT are recognized and honored.

The backup file value is not retrieved, and the current setting remains valid:

- when a value in the backup file has changed and
- that value corresponds to an application that OPSTAT indicates should not be changed.

This prevents a user from bypassing the administration of OPSTAT and changing options settings in the backup file.

Note:

If you administered the APPSTAT parameter to suppress changes to one or more applications, the telephone backs up and restores data as usual, but ignores data for “suppressed” applications. This prevents a user from bypassing your APPSTAT restrictions by editing the backup file. For information about APPSTAT, see The Application Status Flag (APPSTAT) on page 84.

During backup file restoration, user activity is prohibited until a `Restore successful` or `Restore Failed` message displays. When a restore attempt fails, if a retrieved file has no valid data, or if a retrieved file cannot be successfully stored, a `Retrieval Failed` message displays at the telephone until the user takes another action.

Data retrieval considerations are as follows:

- When you create a backup file rather than edit an existing one, be sure to create the file with UTF-16 LE (little endian) characters, with Byte Order Mark (BOM) for LE of 0xFFFE.
- Backup saves data values using the generic format *name*=*value*. For specific formats, see Backup.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, but the case of parameter values, Contact names, and numbers is preserved.
- Spaces preceding, within, or following a *name* are treated as part of the *name*.
- <CR> and <LF> (UTF-16 characters 0x000D and 0x000A, respectively) are interpreted as line termination characters.
- Blank lines are ignored.
- When an identifier is not recognized or is invalid, the entire line is ignored. Likewise, if an identifier is valid but the data itself is invalid or incomplete, the line is ignored.
- When an identifier is valid with valid and complete data, but the data is not applicable to the current state of the telephone, the data is retained for possible use later, and is considered data to be backed up at the appropriate time. For example, if button labels for an SBM24 button module unit are present, but no such module is attached to the telephone, the button labels are retained.
- When more than one line contains a value for an option, parameter, or Contacts entry, the last value read is retrieved, to allow new values to overwrite previous values as lines are read from the backup file. In all other cases, the line order in the backup file has no bearing on retrieval.
- The existence of invalid data does not constitute a failed retrieval. The success of the retrieval process requires the telephone to obtain the backup file and successfully restore valid data.

Chapter 8: Administering Applications and Options

Customizing 9600 Series IP Telephone Applications and Options

The 9600 Series IP Telephones have some unique and powerful capabilities that take advantage of their display and access to LAN facilities. If your LAN has a WML Web site, the telephone needs key information about the servers providing those facilities. You need to provide the information called for in relevant sections of Table 12 in a customized script file. For more information, see 9600 Series IP Telephone Scripts and Application Files on page 54.

CAUTION:

For the telephones to work properly, you must have a *46xxsettings.txt* file in the same directory as the application file. If you do not edit the 46xxsettings.txt file, those telephones use default settings only. The 46xxsettings file is available as a standalone download. If you already have such a file because you downloaded it for a previous 9600 Series or 4600 Series IP Telephone release, installing the standalone file overwrites the original file.

Note:

To facilitate administration, the 9600 Series and 4600 Series IP Telephones use the same ***46xxsettings.txt*** file.

In Table 12, parameters shown with a **Mandatory** status must be accurate and non-null for the application to work. You can change parameters with an **Optional** status to suit your environment. If you do not change parameters, the defaults are used.

Table 12: 9600 Series IP Telephone Customizable System Parameters

Parameter Name	Default Value	Status	Description and Value Range
General User Parameters:			
APPSTAT	1	Optional	Applications status flag. See The Application Status Flag (APPSTAT) on page 84 for a description. See Table 13 for the range of values.
OPSTAT	111	Optional	Options status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as noted in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = setting for Logout application, if applicable. The binary "0" does not allow an end user to see or invoke options and related applications. The binary "1" allows full display and access to all options and related applications.

1 of 3

Table 12: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Web Access Application Parameters:			
SUBSCRIBELIST	" " (Null)	Optional	Subscription list for potential pushed content. List of zero or more fully qualified URLs, separated by commas without intervening spaces, with up to 255 total characters.
TPSLIST	" " (Null)	Optional	List of Trusted Push Servers. List of zero or more fully qualified domain/path strings, separated by commas without intervening spaces, with up to 255 total characters. For more information, see the *4600 Series IP Telephone Application Programmer Interface (API) Guide* (Document Number 16-300256).
WMLHOME	" " (Null)	Mandatory	Text string containing the URL of the home page for the Web Access application.
WMLPROXY	" " (Null)	Optional	Text string containing the IP address, in dotted decimal or DNS format, of an HTTP proxy server. This parameter is optional if the Web pages a user accesses are all on the intranet of your organization.
WMLEXCEPT	" " (Null)	Optional	Text string containing a list of one or more HTTP proxy server exception domains, separated by commas, up to a total of 127 ASCII characters. This parameter is optional if the Web pages to be accessed by the user are all on the intranet of your organization. If WMLPROXY is null, the value of this parameter is ignored.
WMLPORT	80	Optional	Text string containing the TCP port number for the HTTP proxy server. The default is the TCP default for HTTP. This parameter is optional if the Web pages to be accessed by the user are all on the intranet of your organization. If WMLPROXY is null, the value of this parameter is ignored.

2 of 3

Table 12: 9600 Series IP Telephone Customizable System Parameters (continued)

Parameter Name	Default Value	Status	Description and Value Range
Backup/Restore Parameters			
BRURI	" " (Null)	Mandatory	URL used for backup and retrieval of user data. Specify HTTP server and directory path to backup file. Do not specify backup file name. Value: 0-255 ASCII characters. Null is a valid value and spaces are allowed. If this value is null or begins with a character sequence other than *http://* or *https://* the Backup/Restore option will not display to the telephone user.
Backlight Parameters			
BAKLIGHTOFF	120	Optional	Number of idle minutes after which the backlight turns off (1-3 ASCII digits, from 0-999).

3 of 3

Note:

The *4600 Series IP Telephones Application Programmer Interface (API) Guide* (Document Number 16-300258) provides assistance in developing local Web sites.

The Application Status Flag (APPSTAT)

The 9600 Series IP Telephones offer the user numerous applications like Contacts, Call Log, Redial, and so on. Each of these applications allows the user to add, delete, or in some cases, edit entries. You, as the administrator, might not want the user to have that level of functionality. For example, a hotel lobby telephone probably should not allow a user to delete the concierge's contact number. Further, for privacy reasons, that same telephone should not allow a Call Log display. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more telephones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero ("0") value is the most limiting setting. Values "2" and "3" allow increasing levels of functionality, and "1" allows the user complete application functionality.

Table 13: Application Status Flags and Their Meaning

APPSTAT Value	Meaning
0	Redial and Call Log are suppressed. Contact changes are not allowed.
1	***All administered applications are displayed, with full functionality. This is the default value.***
2	Call Log is suppressed. Contact changes are not allowed. Only one-number Redial is allowed.
3	Contact changes are not allowed.

In Table 13, “suppressed” applications are not displayed to the user. Softkey labels, application tabs, and so on are not labeled or displayed. Options associated with suppressed applications can continue to display unless you override them by appropriate OPSTAT parameter administration. Displayed options have no effect while the application is suppressed.

In Table 13, “Contact changes are not allowed” means the Contact application displays and the user can make calls as normal. Any controls that allow the user to change any aspect of the Contact application do not display. This restriction includes the ability to add, delete, or edit any Contact name or number.

In Table 13, “Only one-number Redial is allowed” means the user Option that allows a choice between displaying last numbers dialed is suppressed. The Redial buffer stores only one number. The Redial application does not display since the user can redial only one number. This restriction allows privacy once a given user has left the telephone.

You can:

- set **APPSTAT** to **1**, for example, in a staging area,
- administer a given telephone with Contact entries of your choice, like the **Concierge telephone number** button in the earlier example,
- then move the telephone to where it will be used, where you have administered APPSTAT to be, for example, 0 (zero).

When the relocated telephone resets, it retains its Contact entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the telephone does not accept any Contact button label changes that might have been made directly on a backup file. Only the existing labels of the telephone are used. This restriction prevents circumvention of the APPSTAT restrictions. The WML applications are also suppressed by default.

Appendix A: Glossary of Terms

802.1D 802.1Q	802.1Q defines a layer 2 frame structure that supports VLAN identification and a QoS mechanism usually referred to as 802.1D.
802.1X	Authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access. Applicable 9600 Series IP telephones support IEEE 802.1X for pass-through and for Supplicant operation with the EAP-MD5 authentication method.
ARP	Address Resolution Protocol, used, for example, to verify that the IP address provided by the DHCP server is not in use by another IP telephone.
CELP	Code-excited linear-predictive. Voice compression requiring only 16 kbps of bandwidth.
CLAN	Control LAN, type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP address allocation and management.
DiffServ	Differentiated Services, an IP-based QoS mechanism.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used wherever IP addresses were available as long as a valid DNS server is identified first.
Gatekeeper	H.323 application that performs essential control, administrative, and managerial functions in the media server. Sometimes called CLAN in Avaya documents.
H.323	A TCP/IP-based protocol for VoIP signaling.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
LAN	Local Area Network.
MAC	Media Access Control, ID of an endpoint.
Media Channel Encryption	Encryption of the audio information exchanged between the IP telephone and the call server or far end telephone.
NAPT	Network Address Port Translation.

1 of 2

NAT	Network Address Translation.
OPS	Off-PBX Station.
PHP	Hypertext Preprocessor, software used to assist in the format and display of Web pages.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
QoS	Quality of Service, used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSVP	Resource ReSerVation Protocol, used by hosts to request resource reservations throughout a network.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.
Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.
SIP	Session Initiation Protocol. An alternative to H.323 for VoIP signaling. This protocol is not applicable to 9600 Series IP Telephones.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
UDP	User Datagram Protocol, a connectionless transport-layer protocol.
Unnamed Registration	Registration with Avaya Communication Manager by an IP telephone with no extension. Allows limited outgoing calling.
VLAN	Virtual LAN.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
WML	Wireless Markup Language, used by the 9600 Series IP Telephone Web Browser to communicate with WML servers.

2 of 2

Appendix B: Related Documentation

IETF Documents

The following documents provide standards relevant to IP Telephony and are available for free from the IETF Web site: http://www.ietf.org/rfc.html.

- *Requirements for Internet Hosts - Communication Layers*, October 1989, by R. Braden (STD 3: RFC 1122)
- *Requirements for Internet Hosts - Application and Support*, October 1989, by R. Braden (STD 3: RFC 1123)
- *Internet Protocol (IP)*, September 1981, by Information Sciences Institute (STD 5: RFC 791), as amended by *Internet Standard Subnetting Procedure*, August 1985, by J. Mogul and J. Postel (STD 5: RFC 950)
- *Broadcasting Internet Datagrams*, October 1984, by J. Mogul (STD 5: RFC 919)
- *Broadcasting Internet Datagrams in the Presence of Subnets*, October 1984, by J. Mogul (STD 5: RFC 922)
- *User Datagram Protocol (UDP)*, August 28, 1980, by J. Postel (STD 6: RFC 768)
- *Transmission Control Protocol (TCP)*, September 1981, by Information Sciences Institute (STD 7: RFC 793)
- Domain Names - Concepts and Facilities (DNS), November, 1987, by P. Mockapetris (STD 13: RFC 1034)
- Domain Names - Implementation and Specification (DNS), November 1987, by P. Mockapetris (STD 13: RFC 1035)
- *An Ethernet Address Resolution Protocol (ARP)*, November 1982, by David C. Plummer (STD 37: RFC 826)
- *Dynamic Host Configuration Protocol (DHCP)*, March 1997, by R. Droms (RFC 2131)
- *DHCP Options and BOOTP Vendor Extensions*, March 1997, by S. Alexander and R. Droms (RFC 2132)
- *RTP: A Transport Protocol for Real-Time Applications (RTP/RTCP)*, January 1996, by H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson (RFC 1889)
- *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (DIFFSRV)*, December 1998, by K. Nichols, S. Blake, F. Baker and D. Black (RFC 2474)

- *Management Information Base for Network Management of TCP/IP Internets: MIB-II,* March 1991, edited by K. McCloghrie and M. Rose (RFC 1213)
- *SNMPv2 Management Information Base for the Internet Protocol using SMIv2,* November 1996, edited by K. McCloghrie (RFC 2011)
- *Structure of Management Information Version 2 (SMIv2),* April 1999, edited by K. McCloghrie, D. Perkins, and J. Schoenwaelder (RFC 2578)
- *Resource ReSerVation Protocol VI*, September 1997, by R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin (RFC 2205)
- *The TLS Protocol Version 1.0,* January 1999, by T. Dierks and C. Allen (RFC 2246)

ITU Documents

The following documents are available for a fee from the ITU Web site: http://www.itu.int**.**

- *Recommendation G.711, Pulse Code Modulation (PCM) of Voice Frequencies*, November 1988
- *Recommendation G.722, 7 kHz Audio-Coding within 64 kbit/s*, November 1988
- *Recommendation G.729, Coding of speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP)*, March 1996
- *Annex A to Recommendation G.729: Reduced complexity 8 kbit/s CS-ACELP speech codec*, November 1996
- *Annex B to Recommendation G.729: A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70*, November 1996
- *Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communications systems*, February 1998
- *Recommendation H.245, Control protocol for multimedia communication*, February 1998
- *Recommendation H.323, Packet-based multimedia communications systems*, February 1998

ISO/IEC, ANSI/IEEE Documents

The following documents are available for a fee from the ISO/IEC standards Web site: http://www.iec.ch.

- *International Standard ISO/IEC 8802-2:1998 ANSI/IEEE Std 802.2, 1998 Edition, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks- Specific requirements- Part 2: Logical Link Control*
- *ISO/IEC 15802-3: 1998 ANSI/IEEE Std 802.1D, 1998 Edition, Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Common specifications- Part 3: Media Access Control (MAC) Bridges*
- *IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*
- *IEEE Std 802.3af-2003, IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements- Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications- Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)*
- *IEEE Std. 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control.* For more information about 802.1X, see: http://www.standards.ieee.org/getieee802/download/802.1X-2004.pdf

Index

Numerical

802.1X 69
9600 Series IP Telephones
Administering Options for 59
Administration Alternatives and Options 12
Customizable System Parameters 60
Customizing Applications and Options 81
General 11
Initialization Process 16
Network Audio Quality Display 24
Scripts and Application Files 54

A

About This Guide 7
Administering Applications and Options 81
Administering Avaya Communication Manager 29
Administering Telephone Options 59
Administration Alternatives and Options for 9600 Series IP Telephones 12
Administration Overview and Requirements 11
Administration, for Avaya Communication Manager . 29
Administration, for Telephones on media server . . . 34
Administrative Checklist 15
Administrative Options, Local 71
Administrative Process, The 14
Aliasing 29
Alternatives, Administration 12
ANSI/IEEE Documents 91
Application File and Upgrade Script, Choosing 54
Application Files and Telephone Software 53
Application Files, and Scripts for 9600 Series IP Telephones 54
Application Status Flag (APPSTAT) 84
Application Status Flags and Their Meaning 85
Applications and Options, Administering 81
Applications Diagram 27
Applications, Customizing 81
Application-specific parameters, administering 13
APPSTAT 84
Assessment, of Network 19

B

Backup 77
Backup File Formats 77
Backup, Options and Non-Password Parameters Saved 78
Backup/Restore 76
Backup/Restore HTTP Configuration 48

C

Call Server Requirements 29
Call Transfer Considerations 32
Checklist, Administrative 15
Communication Manager Administration 29
Conferencing Call Considerations 33
Contents of the Settings File 56
Customizable System Parameters 60
Customizing 9600 Series IP Telephone Applications and Options 81

D

DHCP and File Servers 35
DHCP Generic Setup 36
DHCP options 37
DHCP Server 20
DHCP Server Administration 36
DHCP Server Setup 36
DHCP Server to Telephone initialization 17
DHCP Server, Windows 2000 Setup 44
DHCP Server, Windows NT 4.0 Setup 40
DIFFSERV 32
DNS Addressing 68
Document Organization 10
Documentation, Related 10, 89

E

Enhanced Dialing Procedures 74
Enhanced Local Dialing 74
Error Conditions 18

F

File download
Choosing the Right Application and Upgrade Script File 54
Download File Content 54

G

General Download Process 53
Generic Setup, for DHCP 36
Glossary of Terms 87
GROUP System Value 57

H

Hardware Requirements 19
HTTP Configuration for Backup/Restore 48
HTTP/HTTPS Server 20

I

IEC/ISO Documents 91
IEEE 802.1D and 802.1Q 23, 31
IEEE 802.ID/Q QoS parameters 31
IEEE/ANSI Documents 91
IETF Documents 89
Initialization and Address Resolution Diagram 27
Initialization Process, for 9600 Series IP Telephones . 16
Installation, Network Information Required before installing 21
Interface, administering the 13
IP Address Lists and Station Number Portability . . . 24
IP Addresses, administering 12
IP Interface and Addresses, for media servers 30
ISO/IEC, ANSI/IEEE Documents 91
ITU Documents 90

L

Language Selection 72
Local Administrative Options 71

M

Media Server (Switch) Administration 30
Media Server Administration, Other Considerations . 32
Media Server Field Names and Corresponding Script File Parameter Names 50

N

NAT 32
Network Assessment 19
Network Audio Quality Display 24
Network Considerations, Other 22
Network Information, Required 21
Network Requirements 19

O

Options and Applications, Administering 81
Options, Administering 59
Options, Customizing 81
Options, entering using the Telephone Dialpad 71
Options, for 9600 Series IP Telephone Administration . 12
Other Considerations for Administering 9600 Series IP Telephones on Avaya Media Servers . . . 34
Other Considerations, for media server administration 32
Other Network Considerations 22

P

Parameter Data Precedence 14
Parameters in Real-Time 24
Parameters Saved During Backup 78
Parameters, Customizable 60, 82
Pass-Through and Proxy Logoff, 802.1X 69
Port Utilization
  Selection 30
  TCP/UDP 25
Proxy Logoff and Pass-Through, 802.1X 69

Q

QoS 23, 31
  Administrative Parameters 13
  IEEE 802.1D and 802.1Q 31

R

Registration and Authentication 28
Related Documentation 89
Reliability and Performance 23
Requirements 11
  Call Server 29
  Hardware 19
  Network 19
  Server 20
Restore 78
Restore/Backup 76
RSVP and RTCP 31
RTCP and RSVP 31

S

Script File Parameter Names and Corresponding Media Server Field Names 50
Scripts and Application Files, for 9600 Series IP Telephones 54
Security 28
Server Administration 35

Server Administration, DHCP 36
Server Requirements. 20
Settings File 55
Settings File, Contents 56
SNMP. 22
Software 53
Software Checklist 35
Software, Telephone 53
Station Number Portability and IP Address Lists . . . 24
Supplicant Operation, 802.1X. 70
Switch Administration 30
Switch Compatibility and Aliasing IP Telephones. . . 29
System Parameters, Customizable 60, 82

T

Tagging and VLAN, administering. 12
TCP/UDP Port Utilization 25
Telephone Administration 12, 34
Telephone Administration, Other Considerations. . . 34
Telephone and Call Server initialization 17
Telephone and File Server initialization 17
Telephone Initialization Process 16
Telephone Options, Administering 59
Telephone Software and Application Files 53
Telephone to Network initialization 16
Terms, Glossary of. 87

U

UDP Port Selection 30
UDP/TCP Port Utilization 25
Unnamed Registration 18
Upgrade Script and Application File, Choosing the Right 54
Upgrade Script File 54
Upgrade Script, contents of 56

V

VLAN Considerations 66
VLAN Default Value 66
VLAN Separation 67
VLAN Separation Rules 67
Voice Mail Integration 32

W

Web Configuration Tool 50
Web Server 20
What's New 9